Elftes Zürcher Präventionsforum : Neue Technologien im Dienste der Prävention: Möglichkeiten - Risiken

Cavelti, Ladina ; Stössel, Jasmine ; Blanke, Ulf ; Zahnd, Bettina ; Wenk, Thomas ; Schimpel, Ulrich

Abstract: Der technische Fortschritt schafft neue Gelegenheiten für Kriminalität. Man denke nur an Hacking, Datenbeschädigung, Trojanische Pferde und andere Schadsoftware im Internet. Auch im Alltag werden immer häufiger technische Hilfsmittel zu kriminellen Zwecken eingesetzt, wie beispielsweise Drohnen mit hochauflösenden Kameras, Miniwanzen und andere Sensoren zur Aufzeichnung von vertraulichen Bildern und Ton. Die Technik ist aber auch ein Hilfsmittel für die Kriminalprävention. Zu nennen sind etwa bauliche Massnahmen an Häusern, Videoaufzeichnungen in Trams, Bussen oder der Eisenbahn, automatische Suchläufe nach illegalen Inhalten im Internet, Aufklärungsdrohnen, elektronische Fussfesseln und Apps zur Registrierung von verdächtigem Verhalten. Sie alle können zur Verhinderung von Straftaten und zur Beweissicherung eingesetzt werden. Mit der zunehmenden Verfügbarkeit von Daten sind auch neue Auswertungsmethoden (machine learning, big data analysis) möglich, die zu individuellen oder räumlichen Prognosen eingesetzt werden. Das neue Zauberwort lautet: Computational Criminology. Diese Sammlung von Aufsätzen beschreibt die Vielfalt der Einsatzmöglichkeiten neuer Technologie im Dienste der Kriminalprävention. Anwendungsbeispiele erläutern den gegenwärtigen Stand der Umsetzung in der Praxis.

DOI: https://doi.org/10.36862/eiz-286

Other titles: 11. Zürcher Präventionsforum : Neue Technologien im Dienste der Prävention: Möglichkeiten - Risiken

Originally published at:
Cavelti, Ladina; Stössel, Jasmine; Blanke, Ulf; Zahnd, Bettina; Wenk, Thomas; Schimpel, Ulrich Elftes Zürcher Präventionsforum : Neue Technologien im Dienste der Prävention: Möglichkeiten - Risiken. Edited by: Schwarzenegger, Christian; Nägeli, Rolf (2020). Zürich: EIZ Publishing.
DOI: https://doi.org/10.36862/eiz-286

EuropaInstitut

AN DER UNIVERSITÄT ZÜRICH

Assoziiertes Institut der Universität Zürich & Kooperationspartner der ETH Zürich
RECHT BERATUNG WEITERBILDUNG

Herausgeber:
Christian Schwarzenegger, Rolf Nägeli

Elftes Zürcher Präventionsforum

Neue Technologien im Dienste der Prävention: Möglichkeiten – Risiken

EIZ Publishing

EuropaInstitut

AN DER UNIVERSITÄT ZÜRICH

Assoziiertes Institut der Universität Zürich & Kooperationspartner der ETH Zürich
RECHT BERATUNG WEITERBILDUNG

Herausgeber:
Christian Schwarzenegger, Rolf Nägeli

Elftes Zürcher Präventionsforum

Neue Technologien im Dienste der Prävention: Möglichkeiten – Risiken

EIZ Publishing

Editors: Christian Schwarzenegger, Rolf Nägeli – Europa Institut an der Universität Zürich
Publishing & production: buchundnetz.com
Cover: buch&netz
ISBN: 973-3-03805-286-9 (Print – Hardcover), 978-3-03805-285-2 (Print – Softcover), 978-3-03805-308-8 (PDF), 978-3-03805-309-5 (ePub), 978-3-03805-310-1 (mobi/Kindle)
DOI: https://doi.org/10.36862/eiz-286
Version: 1.21-20200309

Dieses Werk ist als buch & netz Online-Buch und als eBook in verschiedenen Formaten, sowie als gedrucktes Buch verfügbar. Weitere Informationen finden Sie unter der URL: http://buchundnetz.com/werke/eizpraeventionsforum11

Vorwort

Der technische Fortschritt schafft neue Gelegenheiten für Kriminalität. Man denke nur an Hacking, Trojanische Pferde und andere Schadsoftware oder Drohnen und Miniwanzen zur Überwachung und illegalen Aufzeichnung von Bild und Ton. Technik ist aber ebenso ein Hilfsmittel für die Kriminalprävention. Bauliche Massnahmen an Gebäuden, Videoinstallationen in Zügen und Bussen, automatisierte Suchläufe im Internet, Drohnen, elektronische Fussfesseln und Apps auf Mobiltelefonen können zur Verhinderung von Straftaten eingesetzt werden. Analyse-Tools mit Zugriff auf eine Vielzahl an Daten ermöglichen Prognosen über die Kriminalitätsentwicklung. Software mit künstlicher Intelligenz wird auch in der Kriminalprävention zum Einsatz kommen.

Technische Massnahmen sind wesentlicher Bestandteil der Kriminalprävention auf allen Ebenen. Dieser Band bietet einen Überblick über neueste Entwicklungen und die Forschung zur Wirksamkeit technischer Kriminalprävention. Das 11. Zürcher Präventionsforum hatte sich zum Ziel gesetzt, über den Stand der Präventionsmassnahmen im Bereich technische Innovationen und Prävention zu informieren und beste Praktiken aufzuzeigen. Entsprechend geht der vorliegende Band insbesondere folgenden Fragen nach: Welche Massnahmen haben sich in der Schweiz und international als wirksam erwiesen? Welche Gefahren gehen von der technischen Innovation aus? Welche Verbesserungen können mit technischen Massnahmen erzielt werden? Welche Möglichkeiten stehen der Polizei, den Behörden, aber auch den Bürgerinnen und Bürgern zur Verfügung? Wie ist der Stand der technischen Prävention in der Schweiz im Vergleich mit anderen Ländern?

Ladina Cavelti, wissenschaftliche Mitarbeiterin am kriminologischen Institut der Universität Zürich, gibt einen Überblick über die verschiedenen Technologien, die bei Kriminalprävention Anwendung finden und zeigt auf, welche Entwicklungstendenzen sich im positiven wie negativen abzeichnen.

Dr. Jasmine Stössel, ausserordentliche Staatsanwältin des Kantons Schaffhausen, informiert über das Electronic Monitoring im Schweizer Erwachsenenstrafrecht, wobei sie sowohl auf die verschiedenen technischen Möglichkeiten mit ihren Vor- und Nachteilen, als auch auf die verschiedenen Anwendungsbereiche eingeht.

Dr. Ulf Blanke, Co-Founder der Antavi GmbH in Zürich, stellt App gesteuertes Crowd-Management und Einsatzführung bei Grossveranstaltungen vor und erklärt, wie gefährliche Situationen auf diese Weise besonders schnell erkannt und ein frühzeitiges Eingreifen ermöglicht werden können.

Bettina Zahnd, Leiterin der Unfallforschung und Prävention der AXA, Winterthur, erläutert anhand verschiedener Studien die Verkehrsunfallprävention durch Fahrerassistenzsysteme und zeigt auf, welche Vorteile und Risiken mit dieser Technologie einhergehen.

Tomas Wenk, Chef des Kompetenzzentrums Digitale Ermittlungsdienste der Stadtpolizei Zürich, vermittelt einen Einblick in aktuelle Phänomene digitalisierter Kriminalität und der Cyber-Crime Prävention. Er zeigt die Schwierigkeiten, mit denen sich die Ermittler bei der Verfolgung von Cybercrime konfrontiert sehen, auf und erläutert praxisnah das Vorgehen der Zürcher Stadtpolizei im Umgang mit digitalisierter Kriminalität.

Dr. Ulrich Schimpel, CTO beim IBM Schweiz und Mitglied beim IBM CTO Europe Team, informiert darüber, wie künstliche Intelligenz die Polizei bei erfolgreicher Präventionsarbeit unterstützen kann und wo derartige wissensbasierte Systeme bereits verwendet werden.

Für das gute Gelingen der Tagung und der Veröffentlichung dieses Bandes möchten wir herzlich danken: Frau Irina Ruf für die professionelle Organisation und Durchführung der Veranstaltung sowie Frau Sue Osterwalder, Frau Noura Ranja Mourad und Frau Daniela De Marco für die Gestaltung dieses Tagungsbandes.

Zürich, im November 2019

Christian Schwarzenegger, Rolf Nägeli

Inhaltsübersicht

Kriminalprävention durch technische Massnahmen - Überblick, Wirksamkeit und Entwicklungstendenzen

Ladina Cavelti

Inhalt

I. Einleitung

Im chinesischen Gebiet Xinjiang wird die Prävention von Kriminalität, insbesondere von terroristischen Handlungen, extensiv betrieben. Die Sicherheitsbehörden kontrollieren und überwachen die uigurische Bevölkerung auf Schritt und Tritt, zunehmend wird dabei auf technische Massnahmen und Innovationen gesetzt, wie im März 2019 in einem Artikel im Tagesanzeiger Magazin beschrieben wurde.[1] Xinjiang, ein Wüstengebiet und vierzigmal so gross wie die Schweiz, ist technisch hochgerüstet wie sonst kaum ein anderes Gebiet auf der Welt. Die rund elf Millionen Uiguren werden rund um die Uhr und grossflächig von Überwachungskameras gefilmt, auch in privaten Wohnungen und Schulen. Das Überwachungssystem zeichnet Daten aus Telefonanrufen, E-Mails, Chats, Internetseiten und sogar den Stromverbrauch und das Einkaufsverhalten auf. Messer werden verkauft mit eingraviertem QR-Code des Käufers, damit eine sofortige Identifikation möglich ist. Wer an einer Tankstelle Benzin tanken möchte, muss sich zuerst an einem Automaten registrieren mit Ausweis und Gesichtsscan. Die Polizei und Sicherheitsbehörden installieren GPS-Sender in Autos und Bussen. Eine obligatorische App der Regierung kontrolliert alle Kommunikation, ausländische Mail- und Messenger-Anbieter wie WhatsApp sind blockiert. Dank künstlicher Intelligenz und selbstlernenden Algorithmen werden Daten systematisch ausgewertet und bei „verdächtigen Aktivitäten" wie beispielsweise Abweichungen beim Einkaufsverhalten, wird automatisch eine Meldung an die zuständige Polizeistation erstellt.[2]

Die chinesische Bevölkerung scheint diesen „Volkskrieg gegen Terrorismus" zu befürworten. Sie scheinen auch die eigene Überwachung unter anderem durch Videokameras, erheblich ausgebaut unter Präsident Xi Jinping, zu befürworten. Dennoch fürchten sie sich gleichzeitig auch vor den psychischen Folgen der Überwachung und vor Datenleaks.[3]

Nicht nur in China werden technische Massnahmen wie Überwachungskameras zwiespältig bewertet, je nach Situation und Kontext, in welchem die Massnahmen eingesetzt und angewendet werden. Überwachungskameras sind somit ein gutes Beispiel für sogenannte *Dual Use Instrumente*, also für den

---

1 MAASS, 8 ff.

2 Zum Ganzen MAASS, 8 ff.; SMITH FINLEY, 1 ff.

3 <https://www.businessinsider.com/how-china-is-watching-its-citizens-in-a-modern-surveillance-state-2018-4?r=US&IR=T>; <https://www.nzz.ch/meinung/das-moralische-vakuum-fuellen-chinas-technologieglaeubigkeit-ld.1485165>.

„positiven“ und „negativen“ Einsatz der gleichen technischen Massnahme je nach Standpunkt und Wahrnehmung des Nutzens oder der Verhältnismässigkeit. Der Einsatz von Überwachungskameras als Einbruchschutz beim eigenen Wohneigentum wird gemeinhin als positiv und sinnvoll betrachtet, da es zu unserem eigenen Schutz und Vorteil eingesetzt wird. Ähnliche oder gleiche technische Massnahmen, in diesem Beispiel Überwachungskameras, können hingegen auch in einem negativen Sinne verwendet werden, um Personen zu überwachen wie es der uigurischen Bevölkerung in China momentan geschieht. Der Zweck ist sowohl bei dem für uns positiven und negativen Einsatz ähnlich, es geht um Prävention oder Verhinderung von Kriminalität, im aktuellen Beispiel entweder Einbruch- oder Terrorismusprävention mittels technischer Massnahmen.

Der Beitrag beginnt mit einem Überblick, was unter Kriminalprävention durch technische Massnahmen zu verstehen ist und welche Arten technischer Massnahmen unterschieden werden können. Der zweite Teil widmet sich sodann der Wirksamkeit technischer Massnahmen im kriminalpräventiven Rahmen im Allgemeinen und im Detail anhand verschiedenen, zuvor definierten Anwendungsbereiche. Danach wird auf die neue Welt der technischen Kriminalprävention eingegangen und mögliche Entwicklungstendenzen der Kriminalprävention, speziell in Bezug auf technische Massnahmen, aufgezeigt.

II. Technische Massnahmen der Kriminalprävention

In der kriminologischen Forschung gibt es einige Untersuchungen und Evaluationen zur Wirksamkeit von Überwachungskameras, Strassenbeleuchtung, Electronic Monitoring, Body-Cams und verschiedenen Einbruchschutzmassnahmen wie Fensterverriegelungen. Die verschiedenen Massnahmen, welche zur Prävention verschiedener Straftaten eingesetzt werden, werden in der Forschung jedoch nicht unter „technische Massnahmen“ oder „technische Kriminalprävention“ zusammengefasst. Sucht man im Internet beispielsweise nach technischer Kriminalprävention, dann werden einige Seiten verschiedener Polizeistellen und Organisationen, die sich um Kriminalprävention kümmern angezeigt, die zumeist über Massnahmen zum Einbruchschutz oder über die Möglichkeiten von Überwachungskameras in Kleingartenanlagen informieren.[4]

Dementsprechend ist es nicht offensichtlich, welche Präventionsmassnahmen unter den Begriff „technische Massnahmen“ fallen und wie dieser Begriff einzugrenzen ist. Auch der Begriff Kriminalprävention ist nicht klar umrissen, wie

[4] <https://tinyurl.com/y267q89v>.

es möglicherweise den Anschein hat. Obwohl Kriminalprävention eine lange Geschichte hat, ist sie immer noch ein vager und ungenau definierter Gegenstand.[5]

Wie erwähnt sind die Gedanken zur Prävention straffälligen Verhaltens nicht neu. Seit einigen Jahrhunderten macht man sich Gedanken darüber, wie Straftaten verhindert werden können. In früheren Zeiten bestand Kriminalprävention vorwiegend aus harter, vielfach grausamster Bestrafung der Täter.[6] Während früher Kriminalprävention demnach vorwiegend als Abschreckung verstanden wurde, wird heute unter Kriminalprävention jegliche Massnahme gefasst, die den Anspruch hat, die Kriminalitätsraten zu reduzieren, bzw. die erstmalige und/oder wiederholte Deliktbegehung zu unterbinden.[7]

Gemäss Dollinger ist die Notwendigkeit von Prävention in sich evident.[8] Wenn es effektiv möglich sei, ein Übel zu verhindern, bevor es auftritt oder bevor es noch gravierende Intensität erreiche, dann solle man dies tun.[9] Das frühe Verhindern eines Übels wird gemeinhin fraglos als gültig und richtig gesehen und leuchtet jedem ein. Ob es gelungen ist, ein Übel wie Kriminalität zu verhindern oder zu vermindern, ist unter Umständen nicht unmittelbar ersichtlich. Das Auftreten von Kriminalität ist nicht zwingend als Scheitern von Präventionsmassnahmen zu interpretieren, sondern kann auch ein Bedarf nach mehr Prävention signalisieren. Die Wirksamkeit von Kriminalprävention ist folglich nicht immer klar und ersichtlich.[10]

1. Zur Begrifflichkeit technischer Massnahmen

Neue technische Innovationen wurden und werden stetig entwickelt, um Kriminalität zu verhindern. Der technische Fortschritt hat im Laufe der Jahre die Art und Weise, wie wir über Kriminalität denken und welche Anstrengungen unternommen werden um sie zu verhindern, entscheidend beeinflusst.[11] Eine treibende Kraft der Innovation technischer Massnahmen zur Kriminalprävention ist die Überzeugung, dass ohne die Entwicklung neuster technischen Trends in Bezug auf Sicherheit und Schutz die Öffentlichkeit im Nachteil ist, da die „andere Seite" technische Massnahmen einsetzt, um Straftaten zu

5 Kury, 25.
6 Kury, 24.
7 Dollinger, 187; Kaiser, 74.
8 Dollinger, 188.
9 Dollinger, 188.
10 Dollinger, 188.
11 Byrne/Marx, 21.

begehen.[12] Für die Kriminalprävention tun sich somit gänzlich neue Interventionen auf, die ohne technische Massnahmen nicht denkbar wären oder aufgrund fehlender Ressourcen nicht umgesetzt werden können. Dabei darf nicht vergessen werden, dass Nachweise der tatsächlichen Erreichung des Ziels, Kriminalität zu reduzieren oder zu verhindern notwendig sind, um die dafür eingesetzten technischen Massnahmen zu legitimieren.[13]

Im vorliegenden Beitrag liegt der Schwerpunkt auf Strategien oder Massnahmen, welche technische Innovationen oder Massnahmen nutzen, entweder um erstmalige Straftaten zu verhindern oder um Rückfälle von Personen zu verhindern, die sich nicht ausschliesslich auf traditionelle Aktionen stützen.

Gemäss Kett-Straub erschweren die vielfältigen Möglichkeiten technischer Präventionsmassnahmen die Herleitung eines allgemein gültigen theoretischen Bezugsrahmens.[14] Als Grundprinzip technischer Präventionsmassnahmen müsse gelten, dass die „tatsächlichen Bedingungen am Tatort so gestaltet werden, dass die Begehung einer Straftat für den Täter schwieriger, risikoreicher und weniger lohnend erscheint." [15]

Dieser Ansatz beruht auf der sogenannten situativen Kriminalprävention, welche die Prävention nicht direkt an der Person des Täters ansetzt, sondern am Kontext der Straftat, indem eine für die Kriminalität begünstigende Gelegenheitsstruktur aufgebrochen wird.[16] Der Ansatz der situativen Kriminalprävention begründet sich hauptsächlich auf den Erkenntnissen der kriminologischen Konzepte *Routine Activity Approach* und *Rational Choice Theorie*. Der Routine Activity Approach beschreibt Kriminalität als Zusammenspiel von Täter, Ziel und Bewachung und untersucht die Tatgelegenheiten und Viktimisierungsrisiken, die sich aus dem täglichen Leben und den Routinen in der Freizeit, am Arbeitsplatz oder im Urlaub ergeben. Nach diesem Ansatz entsteht kriminelles Verhalten dann, wenn ein potenzieller Täter auf ein potenziell lohnendes Ziel ohne entsprechenden Schutz trifft. Die Rational Choice Theorie ist geprägt von einem Grundsatz des rationalen Handelns und geht von einer rationalen Kosten-Nutzen-Analyse aus. Dieser Ansatz nimmt an, dass ein potenzieller Täter seine Risiken mit den zu erwartenden Gewinnen abgleicht und sich daraufhin für oder gegen eine Tat entscheidet. Die situative Kriminalprävention nutzt die Erkenntnisse aus diesen zwei Konzepten insofern, als sie die Gelegenheiten für Kriminalität reduzieren möchte. Im

12 Hummer/Byrne, 378.

13 Dollinger, 187.

14 Kett-Straub, 112.

15 Kett-Straub, 112.

16 Clarke, 91; Kett-Straub, 112.

Grunde sagt dieser Ansatz aus, dass es einfacher ist, Orte und Gegebenheiten zu ändern, als Personen. Folglich hat angemessener Schutz durch technische und soziale Massnahmen eine grössere präventive Wirkung als ein direkter Einfluss auf die Persönlichkeit oder das Privatleben des Täters. Das Ziel der situativen Kriminalprävention ist, dem potenziellen Täter so wenig Gelegenheit zur Kriminalität wie möglich zu bieten und dadurch Menschen nicht zur Begehung von kriminellem Verhalten zu verleiten.[17] Situative Kriminalprävention fokussiert sich auf die Kriminalitätsverhütung durch die Reduzierung der Zahl der kriminellen Möglichkeiten und durch die Erhöhung des wahrgenommenen Entdeckungsrisikos.[18]

Dieses situationsbezogene Präventionskonzept lässt sich nun auf Kriminalprävention durch technische Massnahmen übertragen: technische Massnahmen erhöhen das Risiko des (potenziellen) Täters, entdeckt zu werden, steigern die Kosten und reduzieren die Erfolgswahrscheinlichkeit der Tat im Sinne des sinkenden Nutzens und Belohnung.[19] Nicht alle technischen Massnahmen zur Kriminalprävention vermögen alle diese Punkte gleichzeitig zu erfüllen, sie erheben allerdings diesen Anspruch auch nicht. Gemeinhin können technische Massnahmen zur Kriminalprävention als eine Art der situativen Kriminalprävention gelten. Es gibt jedoch umgekehrt situative Interventionen der Kriminalprävention, die keine technischen Massnahmen sind. Man denke hier beispielsweise an die Kontrolle von Wohnanlagen durch Sicherheitspersonal, der Eingrenzung von Räumen oder Grundstücke durch Zäune oder das Entfernen von Sitzmöglichkeiten im öffentlichen Raum um der Ansammlung (unerwünschter) Personen entgegenzuwirken.[20]

2. Arten technischer Massnahmen der Kriminalprävention

Technische Massnahmen zur Kriminalprävention können unterschieden werden zwischen material- und informationsbasierten technischen Präventionsmassnahmen.[21] Materialbasierte technische Präventionsmassnahmen, auch *hard technology* genannt, umfassen typischerweise Geräte, Hardware und Ausrüstungen, die zur Prävention von Kriminalität genutzt werden können. Dazu gehören auch die bekannten baulich-technischen Massnahmen, wie bspw. Fensterverriegelungen, oder die allgegenwärtigen Überwachungskameras,

17 Zum Ganzen: Bowers/Guerette, 1318 ff.; Clarke, 6 f.; Tilley/Sidebottom, 4864 ff.

18 Piza et al., 137; Clarke, 22.

19 Kett-Straub, 112.

20 Kunz/Singelnstein, 333.

21 Byrne/Marx, 19.

Metalldetektoren in Schulen, Gepäckkontrollen an Flughäfen, kugelsichere Bankschalter, Wegfahrsperren in Autos und Sicherheitssysteme in Haushalten und Firmen.[22]

Informationsbasierte technische Massnamen, auch *soft technology* genannt, umfassen die strategische Nutzung von Informationen zur Kriminalprävention, wie bspw. die Entwicklung von Risiko-Assessment-Instrumenten und Massnahmen die zur Verbesserung der Leistung der Polizei dienen, wie bspw. Predictive Policing.[23] Zu den Innovationen der informationsbasierten technischen Massnahmen gehören neue Softwareprogramme, Klassifizierungssysteme sowie technische Innovationen und Massnahmen zur Datenweitergabe und Systemintegration.[24] Dank der stetig entwickelnden Möglichkeiten der Datenverarbeitung können mittels erfassten und gespeicherten Daten umfassende Bewegungs- und Persönlichkeitsprofile erstellt werden, anhand welcher Risikoprofile berechnet werden, die als Grundlage für die Prognoseentscheidung darüber dienen, ob eine präventive Massnahme im Sinne eines Eingreifens erforderlich ist oder nicht.[25] Zu den neusten technischen Massnahmen gehören die aktuellste Generation von Instrumenten zur Klassifizierung von Straftätern, Instrumente zur Identifizierung von Mobbing, Softwareprogramme zur Verhinderung von Identitätsdiebstahl und zum Datenschutz, neue Instrumente zur Überwachung der Position und Bewegung von gefährdeten Bevölkerungsgruppen wie Sexualstraftäter.[26]

Die soeben eingeführte Unterscheidung zwischen informations- und materialbasierten Massnahmen verliert jedoch stetig an Relevanz, dank des unaufhaltsamen Fortschrittes der Digitalisierung und der Internet der Dinge. Immer weniger technische Massnahmen zur Kriminalprävention sind rein materialbasierter Natur. Eine Lichtanlage beispielsweise besteht zwar aus physischen Geräten wie den Lampen oder einem Bewegungssensor, was ist aber wenn die Lichtanlage elektronisch, zum Beispiel per Smartphone, gesteuert werden kann? Was, wenn Radarfallen per Software aus einer Zentrale ein- und ausgeschaltet werden können?

3. Überblick über die technischen Massnahmen der Kriminalprävention

Trotz der schwindenden Relevanz der Einteilung in material- und informationsbasierte Arten technischer Massnahmen haben wir versucht, einen Über-

22 Byrne/Marx, 19.

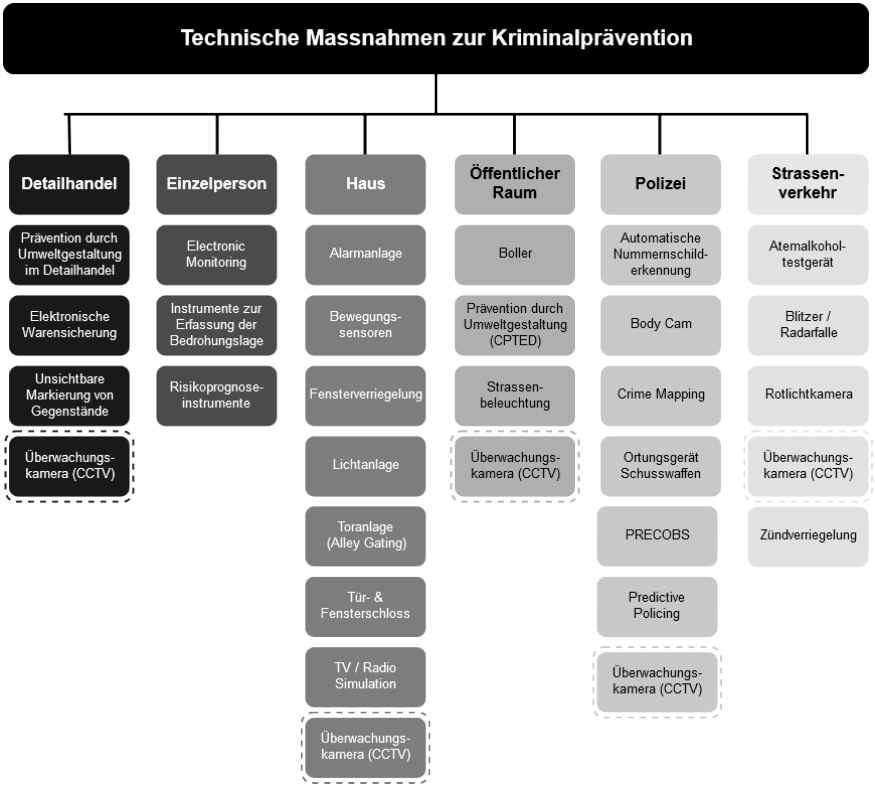
23 Byrne/Marx, 19.

24 Byrne/Marx, 19.

25 Kunz/Singelnstein, 333.

26 Byrne/Marx, 19.

blick über die verschiedenen technischen Massnahmen, die zur Kriminalprävention eingesetzt werden, zu erstellen. Grafik 1 ist das Resultat unserer Überlegungen. Die technischen Massnahmen, welche uns bei der Recherche zum Beitrag wiederholt über den Weg liefen und zu denen auch Literatur oder Studien gefunden werden konnten, sind aufgeführt. Die Aufführung ist nicht erschöpfend, es gibt sicherlich deutlich mehr technische Massnahmen im kriminalpräventiven Bereich.



Grafik 1: "Überblick über die technischen Massnahmen zur Kriminalprävention" (eigene Grafik)

Nachdem bei der Recherche einige technische Massnahmen zusammenkamen, wurden sie in verschiedene Anwendungsbereiche eingeteilt. Die Anwendungsbereiche *Detailhandel*, *Einzelperson*, *Haus*, *Öffentlicher Raum*, *Polizei* und *Strassenverkehr* wurden von uns erstellt. Man sieht in Grafik 1 auch, dass es

technische Massnahmen wie die Überwachungskamera (CCTV) gibt, die in vielen verschiedenen Anwendungsbereichen zum Einsatz kommt. Im vorliegenden Format wurden sie aus diesem Grunde mehrfach aufgeführt.

Zusätzlich ist zu bemerken, dass sowohl die verschiedenen Anwendungsbereiche, wie auch die in den Anwendungsbereichen enthaltenen einzelnen technischen Massnahmen alphabetisch aufgeführt identifiziert und die entsprechenden technischen Massnahmen zugeteilt. Die Reihenfolge der Aufzählung impliziert keine Relevanz oder besondere Bedeutung, der Übersicht wegen wurde eine alphabetische Reihenfolge bevorzugt.

Es ist schwierig, eine genaue Schätzung des Ausmasses zu geben, in welchem jede einzelne technische Massnahme zur Kriminalprävention ein- und umgesetzt wird. Offensichtlich ist jedoch, dass es sich um eine Wachstumsbranche handelt, mit zunehmenden neuen technischen Massnahmen und Möglichkeiten, wie Kriminalität vorgebeugt und verhindert werden soll, sowohl national wie auch international.[27]

III. Wirksamkeit technischer Massnahmen der Kriminalprävention

Wie bereits erwähnt sind und waren technische Innovationen seit jeher treibende Kräfte, die zu Reformen von Kriminalprävention führten. Jedoch wissen wir erstaunlich wenig über das wie und warum gewisse Innovationen oder Massnahmen angewendet werden und welches die intendierten und nicht-intendierten Konsequenzen von technischen Massnahmen sind.[28]

1. Warum ist die Wirksamkeit von Kriminalprävention relevant?

Um entsprechende präventive Massnahmen zu legitimieren, sind Nachweise der tatsächlichen Erreichung dieses Ziels notwendig.[29] Die finanziellen Investitionen in die unterschiedlichen Innovationen und Massnahmen müssen im Sinne eines ökonomischen Umgangs mit öffentlichen Mitteln der Frage der Wirksamkeit kriminalpräventiver Massnahmen eine besondere Bedeutung zukommen.[30] Während in den USA bereits in den 60er Jahren des letzten Jahrhunderts festgelegt wurde, dass 10% der Fördermittel bei unterstützten

27 Byrne/Marx, 30.
28 Byrne/Marx, 17.
29 Dollinger, 187.
30 Kury, 35.

Projekten für eine Evaluation der Projekte verwendet werden müssen, gibt es hierzulande kaum solche Regelungen.[31] In Deutschland, wie auch in der Schweiz, herrscht derweilen ein Mangel an Wirkungsforschung.[32]

2. Welches sind die Voraussetzungen für wirksame Kriminalprävention?

Mehrere Faktoren beeinflussen die Kriterien zur Beurteilung der Qualität der Evaluationsforschung, wie beispielsweise die politischen Rahmenbedingungen, finanzielle Möglichkeiten aber auch wissenschaftliche Unklarheiten darüber ob „nur" randomisierte Studien mit Kontrollgruppen (die gemeinhin als Goldstandard gelten) miteinbezogen werden sollen oder auch Studien, die dies nicht erfüllen.[33] Zudem kann effektive Kriminalprävention gemäss dem niederländischen Forscher de Waard nur unter Mitarbeit von wissenschaftlicher Seite konzipiert werden.[34] Grundlage dafür ist reliables und valides Wissen, das aus bewährten und qualitativ hochwertigen Forschungsergebnissen stammt.[35]

Ansichten über die Art und das Niveau der benötigten Beweise, die für die Feststellung der Wirksamkeit erforderlich sind, sind je nach Entscheidungsträger, Wissenschaftler oder Praktiker unterschiedlich. Angesichts dieser Diskrepanz werden unterschiedliche Kriterien und Überprüfungsverfahren verwendet um festzustellen, was funktioniert und was nicht („What Works?"). Daher kann es durchaus vorkommen, dass eine kriminalpräventive Massnahme oder Richtlinie, von einer Seite als wirksam erfasst wird, von einer anderen Seite als nicht wirksam bewertet wird.[36] Solche Diskrepanzen verunsichern und verwirren natürlich die Öffentlichkeit sowie die politischen Entscheidungsträger und können das Vertrauen in wissenschaftliche Standards und Empfehlungen schlimmstenfalls untergraben. Darüber hinaus gibt es nicht immer besonders hohe Standards in Bezug auf die Strenge der Evaluierungsforschung die erforderlich ist, um eine Intervention als wirksam zu bezeichnen. Das führt dazu, dass kriminalpräventive Massnahmen empfohlen werden, die bei der Umsetzung keine signifikante Kriminalitätsreduktion bewirken dürfte.[37]

---

31 Kury, 35.

32 Kury, 35.

33 Fagan/Buchanan, 623 f.

34 De Waard, 2.

35 De Waard, 2.

36 Fagan/Buchanan, 618.

37 Fagan/Buchanan, 618.

3. Wie kann Kriminalprävention durch technische Massnahmen wirksam sein?

Es gibt verschiedene Arten, wie Kriminalprävention durch technische Massnahmen wirksam sein kann:

Technische Massnahmen erhöhen den Aufwand der Deliktbegehung, es wird schwieriger oder anspruchsvoller, eine Straftat zu begehen oder erfolgreich zu Ende zu führen. Dank einer technischen Massnahme wie bspw. einer Toranlage muss ein potentieller Täter über höhere Mauern klettern.[38]

Technische Massnahmen können das Entdeckungsrisiko drastisch erhöhen. Der gezielte Einsatz von Überwachungskameras kann bspw. helfen, den Täter zu entmutigen und sein Risiko entdeckt zu werden, erhöhen (weitere nicht technische Massnahmen wie tiefe Hecken können das Entdeckungsrisiko noch weiter in die Höhe steigen lassen).

Technische Massnahmen können je nachdem auch die Wahrnehmung potentieller Täter verändern und ihnen das Gefühl geben, eher entdeckt zu werden auch wenn dies nicht mit der Wirklichkeit übereinstimmt. Zudem haben technische Massnahmen eine allgemeine Abschreckungswirkung. Dies zeigt sich bei Blitzeranlagen, wenn nach Implementation generell alle Personen weniger schnell fahren und nicht nur diejenigen Personen, die mit überhöhter Geschwindigkeit unterwegs waren.[39]

Technische Massnahmen können auch die Belohnung oder die Vorteile für Täter verringern, man denke da an Etiketten in Kleidern, die kaputt gehen bei unsachgemässer Entfernung und bspw. Tintenfarbe auslaufen lassen.[40]

Technische Massnahmen können auch zu Verhaltensänderungen führen bei Personen, die nicht eine Straftat begehen oder begehen wollen. Dies wurde bei einer Untersuchung von Toranlagen festgestellt. Die Forscher fanden heraus, dass das Anbringen eines Tores, welches den Zugang zu Wohnanlagen für Nichtbewohner verunmöglichen soll, die Aufmerksamkeit der Anwohner erhöhte und sie sehr darauf bedacht waren, das Tor zu schliessen und zu schauen, welche Personen sich dem Tor nähern.[41]

---

38 Sidebottom et al., Gating Alleys to Reduce Crime, 1 ff.

39 Steinbach/Perkins/Edwards/Beecher/Roberts, 1 ff.

40 Sidebottom et al., A Systematic Review, 1 ff.

41 Sidebottom et al., Gating Alleys to Reduce Crime, 1 ff.

4. Gibt es Einschränkungen betreffend Wirksamkeit der Kriminalprävention?

Natürlich gibt es auch Einschränkungen der Wirksamkeit von kriminalpräventiven Massnahmen. Gitterstäbe an Hausfenstern, welche Diebe fernhalten sollen, können auch verhindern, dass Bewohner im Falle eines Brandes von innen nach draussen in Sicherheit gelangen. Die Verschlüsselung von Informationen bietet Sicherheit, jedoch mit erhöhten Kosten und Erhöhung des Zeitaufwandes für eine Transaktion, ganz zu schweigen von der Sorge um den Verlust des Schlüssels. Technische Massnahmen, die sich an Täter richten, können auch nach hinten losgehen. Fahrzeuge oder elektronische Geräte, die nur durch eine biometrische Kontrolle oder durch einen Code des Besitzers aktiviert werden können, können im schlimmsten Falle zu einer Zunahme von gewalttätigen Auseinandersetzungen führen. Videokameras in Parkhäusern können den Autodiebstahl in Bereiche verlegen, in denen es keine Kameras gibt. Gepanzerte Bankschalter können zwar die Wahrscheinlichkeit eines Diebstahls verringern, aber den Kunden ein ungutes Gefühl geben. Technische Massnahmen können von solch geringer Qualität sein, dass der zusätzliche kriminalpräventive Effekt gar nicht zum Greifen kommt, wie bei einem Türschloss geringer Qualität. Im schlimmsten Fall sind technische Massnahmen defekt (Alarmanlagen, die keinen Alarm auslösen) oder es ist generell die falsche technische Massnahme, um potentielle Täter abzuschrecken.[42]

Aus einem anderen Blickwinkel betrachtet können auch die Befunde aus Evaluationsstudien die Wirksamkeit kriminalpräventiver Massnahmen durch Verzerrung beeinflussen. Da Kriminalität per Definition ein negativ bewertetes soziales Ereignis darstellt, zeigen sich bspw. besondere Schwierigkeiten darin, nicht verzerrte Stichproben zu gewinnen um aus den Antworten der Personen aus der Stichprobe generalisierbare Rückschlüsse zu ziehen. Eine Quintessenz der evidenzbasierten Kriminalprävention ist daher die Forderung nach hochwertigen Studien nach medizinischem Vorbild. Dies würde bedeuten, dass randomisierte Kontrollstudien als qualitativ beste und am aussagekräftigsten gelten, um Wirksamkeiten zu evaluieren.[43]

Man würde denken, dass der klarste und idealste Erfolgsmassstab für die präventive Wirkung einer technischen Massnahme der Rückgang der Kriminalität nach Einsatz der Massnahme wäre. Doch die Messbarkeit derartiger Effekte ist häufig problematisch. Zumeist behilft man sich mit einem Rückgriff auf Sonderauszählungen der Polizeilichen Kriminalstatistik (PKS) in der untersuchten

---

42 Byrne/Marx, 33.

43 Dollinger, 193 f.

Gegend und unternimmt einen einfachen Vorher-Nachher-Vergleich. Doch eine Veränderung der Datenlage im Sinne eines Rückgangs der Straftaten kann nie eindeutig auf den Einsatz verstärkter technischer Sicherungsmassnahmen zurückgeführt werden. Die PKS als Tätigkeitsbericht der Polizei enthält zu viele Verzerrungsfaktoren, als dass sie einzige Grundlage sein kann.[44] Es könnte sich beispielsweise das Anzeigeverhalten oder auch die Kriminalität an sich geändert haben.[45]

Die Wirksamkeit technischer Massnahmen der Kriminalprävention (und nicht nur in Bezug auf Kriminalprävention) können durch viele Faktoren begrenzt oder ausgeglichen werden, auch innerhalb der Polizei, die verschiedene technische Mittel der Kriminalprävention anwendet und implementiert. Gemäss Erkenntnissen, die über den Zusammenhang von Polizeileistungen und dem Einsatz technischer Massnahmen vorliegen, deutet einiges darauf hin, dass die Entwicklung eines besseren Verständnisses für die technischen Massnahmen, ihre Auswirkungen und Optimierung eine wichtige Herausforderung für die Polizeistellen ist, insbesondere für diejenigen Polizeistellen, welche die neuen technischen Massnahmen als Ressourcenmultiplikator nutzen wollen, um Budget- und Personalgrenzen auszugleichen.[46] Die Auswirkungen der Technologie sind komplex und widersprüchlich, und technische Fortschritte führen nicht immer zu einer einfachen Verbesserung der Kommunikation. Darüber hinaus kann die Technologie zwar viele Aspekte des Funktionierens und der Leistung der Polizei verbessern, aber auch andere beeinträchtigen (z.B. können die Meldepflichten neuer IT- und mobiler Computersysteme die Zeit verkürzen, in der die Beamten mit Bürgern interagieren oder andere Arbeiten durchführen).[47] Das soll nicht heissen, dass der technische Fortschritt in der Polizeiarbeit unerwünscht ist und keine Verbesserung bringen wird. Technische Veränderungen können jedoch ohne erhebliche Planung und Aufwand sowie ohne Infrastruktur und Normen, die den Behörden helfen, den Nutzen der Technologie zu maximieren, keine einfachen und wesentlichen Verbesserungen der Polizeileistung bewirken. Eine Strategie zur Technologieanwendung ist daher unerlässlich und sollte eine sorgfältige Prüfung der spezifischen Möglichkeiten beinhalten, wie neue und bestehende Technologien auf allen Ebenen des Unternehmens eingesetzt und genutzt werden können, um Ziele zur Verbesserung von Effizienz und Effektivität zu erreichen.[48]

---

44 Kett-Straub, 126.

45 Kett-Straub, 126.

46 Koper et al., 3.

47 Koper et al., 4.

48 Koper et al., 4.

5. Ausgewählte Befunde der Wirksamkeit technischer Massnahmen

Die einzelnen technischen Massnahmen zur Kriminalprävention sind zu verschieden, als dass allgemein gültige Aussagen zu ihrer Wirksamkeit getroffen werden können.[49] Mit technischen Massnahmen der Kriminalprävention sollen Wohnungseinbrüche, Gewaltdelikte, Laden- und Autodiebstähle verhindert werden, öffentliche Plätze sollen überwacht und Sachbeschädigungen bis hin zu terroristischen Aktionen rechtzeitig erkannt werden. Viele weitere denkbare Einsatzmöglichkeiten sind möglich.[50] Es ist sinnvoller, die einzelnen Massnahmen getrennt zu untersuchen und Schlussfolgerungen betreffend Wirksamkeit zu betrachten. Im Folgenden werden pro Anwendungsbereich eine technische Massnahme und deren Wirksamkeit ausführlicher besprochen.

a) Mehrere Anwendungsbereiche: Überwachungskamera (CCTV)

Überwachungskameras, auch CCTV genannt (CCTV steht für Closed Circuit Television) ist eine optisch-elektronische Überwachung eines meist öffentlichen Raums durch Kameras in einem geschlossenen System (daher Closed Circuit). Geschlossen bedeutet, dass die aufgenommenen Bilder nur einem begrenzten Nutzerkreis zugänglich sind. Die aufgenommenen Bilder werden entweder einer Überwachungszentrale übertragen oder aufgezeichnet.[51] Die Ziele der Videoüberwachung bestehen in der Abschreckung potentieller Täter, in der Erhöhung der Entdeckungswahrscheinlichkeit von Straftaten, bei der Aufklärungsrate von Straftaten und auch in der Verbesserung des subjektiven Sicherheitsempfindens von Bürger.[52]

In den letzten Jahrzehnten hat sich CCTV zu einer weltweit viel verbreiteten Massnahmen der Kriminalprävention entwickelt. Gemäss PIZA, WELSH und FARRINGTON ist der Anstieg auf Grossbritannien zurückzuführen, wo zwischen 1996 bis 1998 drei Viertel des Budgets des Innenministeriums für CCTV bezogene Projekte investiert wurde.[53] Solche politische Entscheidungen erhöhten die Anzahl der Überwachungskameras und -systeme in Grossbritannien dramatisch, von etwa 100 im Jahr 1990 auf mehr als vier Millionen 20 Jahre später.[54] In den letzten ca. zehn Jahren tätigten auch die Behörden in den Ver-

---

49 KETT-STRAUB, 112.

50 KETT-STRAUB, 113.

51 KETT-STRAUB, 123.

52 KUNZ/SINGELNSTEIN, 333.

53 PIZA ET AL., 136.

54 FARRINGTON ET AL., 22.

einigten Staaten sowie in China und in anderen Ländern erhebliche Investitionen in Überwachungskameras und -systeme.[55] Die zunehmende Verbreitung von Überwachungskameras führte an öffentlichen Orten dazu, dass Überwachungskameras von der Öffentlichkeit und Medien mittlerweile kaum beachtet werden, da sie als alltäglich wurden.[56]

Während andere technische Präventionsmassnahmen punktuell Straftaten verhindern oder reduzieren können, kann mit CCTV eine Bandbreite an Straftaten erfasst werden. Die Breitenwirkung von CCTV kann theoretisch vom Verhindern von Delikten gegen Leib und Leben, Eigentumsdelikten, Strassenverkehrsdelikten, Sachbeschädigungen bis hin zu terroristischen Anschlägen reichen.[57]

Über den Nutzen von CCTV gibt es nach wie vor stark divergierende Aussagen, gerne wird ihr das Etikett der Multifunktionalität angeheftet. Die beabsichtigte Wirkung der Videoüberwachung ist zuvorderst die Verhinderung von Kriminalität in dem überwachten Gebiet. Durch die offene Überwachung mittels Kamera (durch Hinweise wie Schilder) wird die Tatsituation aus Sicht des Täters zu seinen Ungunsten verändert. Dieser situationsbezogene Ansatz basiert aber zwingend auf der Annahme, dass sich Menschen für die Begehung einer Straftat bewusst und rational entscheiden.[58] Fraglich ist zudem, ob die Videoüberwachung im Fall eines bereits unmittelbar bevorstehenden Angriffs auf ein Rechtsgut noch präventive Wirkung entfalten kann. Sicherheitspersonal müsste beispielsweise bei einem Gewaltdelikt noch rechtzeitig eingreifen, so dass zumindest schlimmere Verletzungen des Opfers vermieden werden könnten. Personen müssten hierzu in unmittelbarer Nähe des Einsatzortes stationiert sein. Echte Gefahrenabwehr verlangt einen polizeilichen Zugriff im Sekundenbereich. Zu vermuten ist jedoch, dass selbst wenn der Überfall von den Kameras erfasst wird, nicht immer jemand die Aufzeichnung verfolgt oder die zeitliche Spanne, bis dem Opfer geholfen werden kann, zu gross ist.[59]

Über die präventive Wirkung von Überwachungskameras wurde bisher viel geforscht. In knapp 20 Jahren wurden von den Forschern WELSH und FARRINGTON insgesamt drei Meta-Analysen und systematische Übersichtsarbeiten zusammengestellt, was für das Forschungsgebiet Kriminalprävention unge-

55 PIZA ET AL., 136.

56 PIZA ET AL., 136.

57 KETT-STRAUB, 123.

58 KETT-STRAUB, 121 f.

59 KETT-STRAUB, 122.

wöhnlich viel ist.[60] Für die aktuellste Meta-Analyse aus dem Jahr 2019[61] wurden Studien ausgewählt, welche die folgenden vier Kriterien erfüllten: 1) CCTV war der Hauptgegenstand der Intervention. 2) Die Auswertung erfolgte anhand eines Ergebnismass der Kriminalität, sprich messbare Daten zu Kriminalität wie beispielsweis Polizeirapporte. 3) Das Forschungsdesign beinhaltete mindestens eine Vor- und Nachher-Messung von Kriminalität in der Interventions- und vergleichbaren Kontrollgegend. Dies gilt weithin als Mindestanforderung in der Evaluationsforschung. 4) Sowohl die Interventions- wie auch die Kontrollgegend mussten vor Installation der Überwachungskameras mindestens 20 entdeckte Straftaten aufweisen.[62]

In der ersten Meta-Analyse 2002 erfüllten lediglich 24 Studien alle erforderlichen Voraussetzungen, wobei es auch deutlich weniger Untersuchungen über die kriminalpräventive Wirkung von CCTV gab.[63] In der zweiten Meta-Analyse 2009 (durchgeführt von den gleichen Forschern) wurden 93 Studien und Evaluationen zum Thema CCTV und Kriminalprävention gefunden, jedoch erfüllten davon 49 nicht die Anforderungen und lediglich 44 Studien konnten berücksichtigt werden.[64] Für die aktuellste Meta-Analyse und Überblick wurden zusätzlich zu den früheren miteinbezogenen Studien 68 neue CCTV Studien identifiziert, wovon 29 Studien die Anforderungen nicht erfüllten.[65] Dies zeigt, dass nicht nur im Vergleich zu früheren Studien die Qualität der Studien gestiegen ist, sondern auch dass mehr Studien zur Wirkung von CCTV durchgeführt werden. So kommen auch die Autoren der neusten Meta-Analyse zum Schluss, dass die Zunahme der Anzahl der Studien zu einer verbesserten Wissensbasis über die Wirksamkeit von Videoüberwachung führte. Der Umfang und die Qualität der neuen Forschungen über Videoüberwachungen bestätigen diesen Punkt.[66]

Die Ergebnisse der aktuellsten Meta-Analyse von 2019 der zusammengeführten Effekte zeigen, dass CTV mit einem bescheidenen aber signifikanten Rückgang der Kriminalität assoziiert wird. Der Rückgang wird zudem nicht negativ beeinflusst durch
einen Verdrängungseffekt (Verlagerung der Kriminalität an einen anderen Ort).[67]

---

60 Welsh/Farrington, 1 ff; Welsh/Farrington, 1 ff; Piza et al., 1 ff.

61 Vgl. Piza et al., 135–159.

62 Piza et al., 138.

63 Welsh/Farrington, 13.

64 Welsh/Farrington, 721.

65 Piza et al., 139.

66 Piza et al., 147 f.

67 Piza et al., 148.

Ähnlich wie bei den vorherigen Meta-Analysen zu Überwachungskameras stellten auch Piza, Welsh und Farrington die grössten und konsistentesten Effekte von Videoüberwachung in Parkhäusern fest. Dafür gibt es mehrere Gründe: zum einen wurden in beinahe allen Studien zu CCTV in Parkhäusern andere Massnahmen wie Sicherheitspersonal, Beschilderung und verbesserte Beleuchtung eingesetzt. Zum anderen spielt wohl auch die Flächendeckung der Kameras eine nicht unwichtige Rolle. Studien, welche diese Information erwähnten, berichteten nahezu von 100% Abdeckung des Interventionsgebietes durch Überwachungskameras. Die Wirksamkeit von Überwachungskameras scheint mit dem Abdeckungsgrad der Überwachungskameras zu korrelieren, die am höchsten in Parkhäusern ist.[68] Neben der geografischen Lage von Überwachungskameras scheinen strategische Aspekte bei der Implementierung und Umsetzung von Überwachungskameras eine Relevanz aufzuweisen.[69] Kriminalpräventive Programme, die neben der Einzelmassnahme Überwachungskameras weitere Massnahmen oder Interventionen beinhalteten, zeigten höhere Wirksamkeit als einzelne umgesetzte Massnahme. Beispielsweise zeigte sich, dass die Wirksamkeit von Überwachungskameras grösser war, wenn nicht nur aufgezeichnet wurde, sondern wenn aktiv CCTV mit weiteren Massnahmen gekoppelt wurde.[70] Dies deutet darauf hin, dass CCTV als eigenständige (technische) Massnahme zwar wirksam sein kann bei der Prävention von Kriminalität, aber anstatt sich auf eine alleinige Kamerapräsenz zu verlassen, sollte eine aktive Kameraüberwachung eingesetzt werden.[71]

b) Anwendungsbereich „Detailhandel": Elektronische Warensicherung

Elektronische Warensicherungssysteme sollen im Detailhandel Diebstähle verhindern ohne den Kunden zu beeinträchtigen. Die dabei verwendeten Warensicherungsetiketten können vielfältiger Art sein, es gibt Tintensicherungssysteme, deren Kapsel bei unsachgemässem Entfernen platzt oder Plastiketiketten an Kleidern oder Verschlüsse an Flaschen. Weitere Massnahmen sind Magnetstreifen mit Barcodes, mit denen bspw. Bücher in einem Buchladen oder Bibliothek versehen sind. Solche elektronische Warensicherungssysteme bestehen normalerweise aus drei Komponenten: dem elektronischen Etikett, Detektoren (meist beim Ladenausgang stationiert) und einer Steuereinheit. Die Etiketten lösen einen Alarm aus, wenn sie die Detektoren passieren ohne entfernt oder deaktiviert worden zu sein. Warensicherungsetiketten

---

68 Piza et al., 148.

69 Welsh/Farrington, 19 f.

70 Piza et al., 149.

71 Piza et al., 149.

werden vom Detailhandel bevorzugt, da die gekennzeichneten Artikel offen ausgestellt werden können und somit besser zugänglich sind für Kunden sowie Mitarbeiter.[72]

Der erste systematische Übersichtsbericht zur Wirksamkeit elektronischer Warensicherung als technische Massnahme gegen Diebstahl wurde 2017 publiziert.[73] Die Forschungsgruppe um Sidebottom identifizierte über 50 Studien zur Wirksamkeit von Warensicherungsetiketten im Detailhandel, jedoch erfüllten nur acht Studien die Anforderungen zur Inklusion im systematischen Übersichtsbericht. Aufgrund der erheblichen Unterschiede in der Art der installierten Etiketten und der Messung konnte keine Meta-Analyse durchgeführt werden.[74] Auch sonst kämpften die Forscher mit der Schwierigkeit, Aussagen zur Wirksamkeit verschiedener Warensicherungssysteme zu ziehen. Beispielsweise konnten sie nur eine Studie identifizieren, welche die Wirksamkeit von Tintensicherungen untersuchte. Diese Studie war zudem über 20 Jahre alt. Bei den elektronischen Warensicherungsetiketten fanden die Autoren ältere Studien, welche über einen bedeutsamen Effekt der Etiketten in Bezug auf Diebstahl berichtete, neuere Studien jedoch berichteten keine spürbaren Auswirkungen von elektronischen Warensicherungsetiketten auf die Prävention von Diebstahl. Wieder andere Studien kamen zum Ergebnis, dass sichtbarere Etiketten tendenziell mit einem stärkeren Rückgang des Diebstahls verbunden sind als weniger sichtbare Etiketten.[75]

Die Forscher kommen dann auch zum Fazit, dass der Bereich elektronischer Warensicherung bisher nicht ausreichend untersucht wurde. Die Wissenslücke könnte durch mehr und methodologisch bessere Studien behoben werden.[76]

Zu bemerken ist auch, dass sich die Welt des Detailhandels verändert (und verändert hat) und einerseits durch Online-Läden wie auch durch Selbstbedienungskassen sich neue und andere Möglichkeiten für deviantes Verhalten aufgetan haben. Einige der im Übersichtsbericht identifizierten Studien sind älteren Jahrgangs. Unter diesen Umständen können die ausgeführten Ergeb-

---

72 Zum Ganzen: <https://whatworks.college.police.uk/toolkit/Pages/Intervention.aspx?InterventionID=45>; Sidebottom et al., A Systematic Review, 8 f.

73 Sidebottom et al., A Systematic Review, 1 ff.

74 Sidebottom et al., A Systematic Review, 37.

75 Sidebottom et al., A Systematic Review, 38.

76 Sidebottom et al., A Systematic Review, 39.

nisse über die Wirksamkeit alter Studien zwar noch eine gewisse Relevanz haben, doch sind die derzeitigen Detailhändler angehalten, sich auf die spezifischen Umstände der Risiken der Detailhandelskriminalität zu achten.[77]

c) Anwendungsbereich „Haus": Einbruchschutz

Eine Eigenheit technischer Massnahmen im Bereich des Einbruchschutzes ist, dass sich die Massnahmen an die potentiellen Opfer richten und somit bei der Eigenverantwortung der Bürger ansetzen.[78] Polizei und Versicherungen liefern dazu Beratungen und spezifische Öffentlichkeitsarbeit, die Verantwortung für die Implementation liegt jedoch bei der Person mit Wohneigentum (oder bei Personen mit Verantwortung für Wohneigentum).

Einbruchdiebstahl ist ein Delikt, welches verschiedene besondere Merkmale aufweist: Einen Einbruch in die sicher geglaubte eigene Wohnung oder Haus kann bei Opfern schwere und lang anhaltende Folgen hervorrufen, auch wenn die körperliche Integrität nicht beeinträchtigt wurde.[79] Der Einbruchdiebstahl ist zudem ein Delikt, das im Prinzip alle Bevölkerungsschichten treffen kann, wobei die Möglichkeiten, sich selber durch entsprechende technische Massnahmen gegen Einbrüche zu schützen ungleich verteilt sind in der Bevölkerung und von den finanziellen Möglichkeiten der potentiellen Opfer abhängig sind.[80] Eine weitere Besonderheit ist der Umstand, dass dem Einbruchdiebstahl in der kriminologischen Forschung, zumindest im deutschsprachigen Raum, vergleichsweise wenig Aufmerksamkeit gewidmet wird. Es existiert zwar eine grosse Bandbreite an Informationsmaterial, die von Polizeistellen, Versicherungen und weiteren Organisationen herausgegeben werden sowie einige (regional) durchgeführte Studien. Die präventiven Massnahmen werden hingegen kaum systematisch auf ihre Wirksamkeit hin untersucht.[81]

Dies wollte das Deutsche Forum für Kriminalprävention (DFK) 2004 ändern und gab dem renommierten Kriminologen Feltes den Auftrag, eine wissenschaftliche Studie zur Wirksamkeit technischer Einbruchsprävention bei Wohn- und Geschäftsobjekten durchzuführen.[82] Untersucht wurde, wie Präventionsmassnahmen im Zusammenhang mit Einbruchdiebstahlsdelikte gestaltet sein sollte, damit eine optimale Wirkung entfaltet wird.[83]

---

77 SIDEBOTTOM ET AL., A Systematic Review, 43 f.

78 FELTES, 3.

79 FELTES, 21.

80 FELTES, 21.

81 FELTES, 22.

82 FELTES, 3.

83 FELTES, 23.

Bei der Befragung von 27 Tätern, die wegen Einbruchdiebstahl verurteilt wurden, gaben viele Befragte als Grund für die Begehung eines Einbruchsdelikts das geringe Entdeckungsrisiko an. Die meisten der befragten Täter wurden zudem nicht auf frischer Tat ertappt. Feltes kommt zum Schluss, dass eine deutliche Erhöhung des Entdeckungsrisikos sicherlich präventive Wirkungen zeigen würde.[84] Sowohl die befragten Polizisten wie auch die Versicherungsvertreter waren der Auffassung, dass grundsätzlich alle technischen Massnahmen überwindbar sind. Die Installation von technischen Massnahmen wie gesicherte Fenster und Türen wird trotzdem als sehr wichtig erachtet, da diese Massnahmen potentiell die Entscheidung zum Einbruch bzw. zur Auswahl des Objektes relevanten Faktoren wie Lärm, Zeit und Aufwand für oder gegen eine Tat beeinflussen. Gerade bei Zufallstaten scheuen Täter eher Objekte mit guten technischen und mechanischen Sicherungen und versuchen Situationen zu umgehen, wo Lärm entstehen könnte.[85]

Ganz wichtig sei gemäss den Ergebnissen des Berichts der Faktor Zeit im Bereich der technischen Massnahmen. Die meisten Einbrüche, gleich ob Amateur oder Profi-Einbrecher dauern in der Regel nicht länger als 20 Minuten. Kommt der durchschnittliche Einbrecher nicht innerhalb von zwei bis fünf Minuten in das Gebäude, wird die Tatausführung abgebrochen und zum nächsten Objekt gewechselt.[86]

Interessanterweise wurden technische Massnahmen zur Abschreckung von Einbruchdiebstählen von den befragten Tätern kaum erwähnt. Lediglich einer von 27 befragten Tätern gab an, bei sogenannten „Blitzeinbrüchen“ sich durch einbruchhemmende Fenster und Türen abschrecken zu lassen.[87] Die befragten Polizisten im Gegenzug gehen davon aus, dass Alarmanlagen einer hohen abschreckenden Wirkung zukommen. Die Mehrheit der inhaftierten Einbrecher, die befragt wurden, gab jedoch an, dass die Aspekte der Sicherheitsmassnahmen bei der Entscheidung für oder gegen ein Einbruchsobjekt, keine oder nur eine untergeordnete Bedeutung spielt. Zudem berichteten auch viele der Täter, dass Alarmanlagen keine abschreckenden Wirkungen haben und der Alarm häufig einfach ignoriert wird. Dies aufgrund von Erfahrungswissen. Die Befragten wissen, dass ein Alarm nach einer gewissen Zeit abgestellt wird, oder dass ein ausgelöster Alarm nicht gleichzeitig das Eintreffen der Polizei bedeutet. Viele sagten auch, dass es normalerweise kein grösseres Problem sei, Alarmanlagen oder weitere technische Massnahmen ausser Betrieb zu set-

---

84 Feltes, 32 f.

85 Feltes, 38.

86 Feltes, 39.

87 Feltes, 39.

zen.[88] Feltes stellte auch fest, dass viele Täter im Laufe ihrer Karriere ihren Modus Operandi regelmässig dem neusten Stand der Sicherheitsmassnahmen anpassen und sich an gewisse technische Massnahmen gewöhnen.[89] Sie kommen dann auch zum Fazit, dass gute technische Massnahmen zur Prävention von Einbruchsdiebstählen Schutz vor Einbrecher bieten können, bei hochprofessionellen Einbrechern sind technische Massnahmen eher wirkungslos. In manchen Fällen werden gute Sicherheitsausstattungen noch als besondere Herausforderung betrachtet und gelten als zusätzlicher Anreiz zur Tat.[90]

Welche Konsequenzen hat dies für die Prävention? Technische Präventionsmassnahmen beim Einbruchschutz müssen sowohl den planenden wie auch den „spontan" entscheidenden Täter berücksichtigen. Neben technischen Massnahmen wie der Einbau einbruchhemmender Türen oder sicheren Schliesszylinder sollen auch situative Faktoren (Fenster schliessen und Türen abschliessen auch beim kurzzeitigen Verlassen der Wohnung, Nachbarn auf Abwesenheit aufmerksam machen) berücksichtigt werden.[91]

Eine aktuelle Publikation von 2018 aus Grossbritannien kommt zu einem ähnlichen Schluss.[92] Die Interviews mit 22 verurteilten Einbrechern zeigen, dass Einbrecher auf Objekte mit geringer natürlicher Überwachung, einfachen Zugangs- und Fluchtwegen und schlechter physischer Sicherheit an Orten, in welchem es scheinbar wenig Gemeinschaftsgeist gibt, zielen. Jedoch geben praktisch alle Einbrecher an, dass sie von sichtbaren Alarmanlagen (oder Hinweise darauf wie Kleber) nicht abgeschreckt werden, und übermässig sichtbare technische Massnahmen wie Toranlagen und Fenstergitter als Hinweis auf wertvolle Besitztümer betrachten, was solche Objekte in ihren Augen als besonders attraktiv macht. Für die fehlende Wirksamkeit von Alarmanlagen in England und Wales wird von den Forschern um Tseloni angegeben, dass es in Grossbritannien eine grosse Verbreitung von Alarmanlagen gibt, welche auf deren geringe Kosten zurückzuführen sind. Ergo werden oft billigere und minderwertige Alarmanlagen installiert, die aufgrund technischer Probleme nicht auf Einbrüche aufmerksam machen. Vermutet wird auch, dass Alarmanlagen von Nachbarn oder Passanten als Belästigung und Störung empfunden und daher öfters ignoriert werden.[93]

---

88 Feltes, 40.

89 Feltes, 40.

90 Feltes, 41.

91 Feltes, 41.

92 Tseloni/Thompson/Tilley, 1 ff.

93 Tseloni/Thompson/Tilley, 267.

In Grossbritannien ist daher die effektivste Kombination technischer Massnahmen in Bezug auf Schutz, Sicherheit und Kosten Fensterverriegelungen, Lichtanlagen im Innern des Hauses, Doppeltürverriegelung, Deadlocks und Aussenbeleuchtung mit Bewegungsmelder und Riegelschloss. Die Basis aller wirksamen Sicherheitsmassnahmen sind Fenster- und Doppeltürverriegelung.[94]

d) Anwendungsbereich „Öffentlicher Raum": Strassenbeleuchtung

Eine verbesserte Strassenbeleuchtung dient vielen Zwecken, nicht zuletzt der Kriminalprävention. Während dem die Optimierung von Strassenbeleuchtungen nicht oft mit dem erklärten Ziel der Kriminalprävention verwirklicht werden – Fussgänger- und Verkehrssicherheit werden wohl zumeist als wichtigere Ziele betrachtet – und der Gedanke der Beleuchtung von Strassen als Abschreckungsmassnahme von lauernden Kriminellen zu simpel erscheinen mag, wird die Relevanz verbesserter Strassenbeleuchtung in städtischen Zentren, Wohngebieten und anderen Orten mit hoher Frequenz von Opfern, in der Wissenschaft öfters thematisiert.[95]

Es gibt hauptsächlich zwei Erklärungsansätze darüber, warum eine optimierte Strassenbeleuchtung zu einer Verringerung von Kriminalität führen kann. Zum einen deutet einiges darauf hin, dass eine verbesserte Beleuchtung zu einer verstärkten Wahrnehmung potentieller Täter führt, sowohl durch die verbesserte Sichtbarkeit wie auch durch die erhöhte Anzahl von Personen auf der Strasse, was zu einer stärkeren Abschreckung von potentiellen Tätern führen kann. Zum anderen kann eine verbesserte Strassenbeleuchtung eine Investition der öffentlichen Behörden in die Gegend signalisieren, was zu mehr Gemeinschaftsgefühl und Zusammenhalt und informeller sozialer Kontrolle führen kann. Durch die zweite Theorie würde Kriminalität nicht nur während der Nacht zurückgehen, sondern auch tagsüber. Der von WELSH und FARRINGTON[96] veröffentlichen Übersichtsbericht aus dem Jahre 2008 kam zum Ergebnis, dass eine verbesserte Strassenbeleuchtung tatsächlich Kriminalität verringert und neben den Überwachungskameras eine der wirksameren technischen Massnahmen zur Kriminalprävention im öffentlichen Raum darstellt. Die Auswertungen zeigen auch, dass der Rückgang der Kriminalität nicht nur auf die Nacht beschränkt ist, sondern auch tagsüber abnimmt.[97] Die Forscher

---

94 TSELONI/THOMPSON/TILLEY, 267.

95 WELSH/FARRINGTON, 2.

96 Anmerkung: Die gleichen Forscher, die sich vor allem im Bereich der Wirksamkeitsforschung von Überwachungskameras (CCTV) einen Namen gemacht haben.

97 WELSH/FARRINGTON, 3.

kritisieren jedoch die spärlich vorhandene Menge an Untersuchungen, gerade einmal 13 Studien erfüllten die Anforderungen um in den Übersichtsbericht aufgenommen zu werden. Weitere 19 Studien erfüllten hingegen die Anforderungen nicht weil sie entweder kein Kontrollgebiet (sondern nur ein Interventionsgebiet) untersuchten oder die Anzahl der tatsächlich erfolgten Straftaten zu gering war oder Kriminalität nicht gemessen wurde sondern ein anderes Konstrukt, wie bspw. Kriminalitätsfurcht.[98]

Ob (verbesserte) Strassenbeleuchtung als technische Massnahme zur Kriminalprävention geeignet ist, hängt von den situativen Merkmalen und anderen gleichzeitig durchgeführten technischen und nicht technischen Massnahmen ab.[99] Die im Übersichtsbericht präsentierten Ergebnisse verschiedener Studien zeigen, dass eine verbesserte Strassenbeleuchtung unter bestimmten Umständen ein effektives Mittel sein kann, um Kriminalität zu reduzieren. Was genau diese bestimmten Umstände sind, kann nicht eindeutig beantwortet werden aufgrund der bisher vorhandenen wissenschaftlichen Untersuchungen.[100] WELSH und FARRINGTON schreiben auch, dass sei Aufgabe für zukünftige Evaluationsforschungen.[101] Der Bericht wurde vor mehr als 10 Jahren publiziert, seither wurde im internationalen Forschungsgebiet der Kriminalprävention nicht viel Augenmerk auf Strassenbeleuchtung gelegt.

e) Anwendungsbereich „Polizei": Ortungsgerät für Schusswaffen

Die rasanten Entwicklungen in der Technologie veranlasst nicht nur die Polizei dazu, neue technische Massnahmen zur Bekämpfung und Prävention von Gewaltverbrechen einzuführen. *Gunshot Detection Technology* oder Ortungsgerät für Schusswaffen ist eine relativ neuartige technische Massnahme, die vor allem in Nordamerika zur Anwendung kommt.[102] Das akustische und optische Überwachungssystem, welches vor allem in sogenannten „high crime" Gebieten Einsatz findet, informiert die Polizei in Echtzeit über Schussabgaben, auch wenn weder Polizei noch Sanität via Notruf alarmiert wurden, indem die Daten an eine zentrale Verarbeitungsstelle gesendet werden. Mit Hilfe der GPS-Technologie und den weiteren gesammelten Daten kann das Ortungsgerät unmittelbar Informationen zum Standort der Schussabgabe und auch zum verwendeten Waffentyp liefern. Diese Informationen können bis zu 20 Sekunden nach dem Erkennen des Schusses eintreffen. Sobald die Informatio-

98 WELSH/FARRINGTON, 8; WELSH/FARRINGTON, 37.

99 WELSH/FARRINGTON, 23.

100 Welsh/Farrington, 23.

101 WELSH/FARRINGTON, 23.

102 CHOI/LIBRETT/COLLINS, 48.

nen von der Polizeistation empfangen werden, können Polizisten zum Tatort geschickt werden, was der Polizei ermöglicht, rasch vor Ort zu sein und falls notwendig, eingreifen zu können.[103]

f) Anwendungsbereich „Strassenverkehr": Geschwindigkeitsüberwachung (Blitzeranlage)

Die Überschreitung von Höchstgeschwindigkeiten kann schwerwiegende Folgen nach sich ziehen. Bei höheren Geschwindigkeiten sind die Reaktions- und Bremswege länger, was die Wahrscheinlichkeit von Verkehrsunfällen erhöht.[104] Geschwindigkeitsbegrenzungen dienen der Regulation des Verkehrs durch die Festlegung einer sicheren Obergrenze für Fahrzeuggeschwindigkeiten. Zu den technischen Massnahmen zur Durchsetzung von Geschwindigkeitsbegrenzungen im Strassenverkehr gehört u.a. der Einsatz von sogenannten Blitzeranlagen. Neben technischen Massnahmen gibt es auch Massnahmen, die darauf abzielen das Bewusstsein des Fahrers für Sicherheitsfragen in Bezug auf Geschwindigkeitsübertretungen zu sensibilisieren.[105]

Einen systematischen Überblick über die präventive Wirksamkeit von Blitzeranlagen wurde 2016 in Grossbritannien publiziert.[106] 51 Studien wurden dafür systematisch erfasst und ausgewertet. Über alle Studien hinweg gesehen führte die Implementation von Blitzeranlagen zu einer Verringerung der Durchschnittsgeschwindigkeit der gemessenen Fahrzeuge um 7%, Unfälle gingen durchschnittlich um 19% zurück und Unfälle mit Verletzungsfolgen um 18%.[107] Dabei macht es keinen Unterschied, welche Art von Blitzer (stationär oder mobil) eingesetzt wurde und es gibt keine Hinweise auf den Unterschied der Wirkung zwischen sichtbaren oder verdeckten Kameras.[108]

Der Bericht liefert Beweise dafür, dass Blitzer eine wirksame technische Massnahme zur Reduzierung des Geschwindigkeitsverhaltens sind und dazu beitragen können, einige der negativen Folgen der Geschwindigkeitsübertretungen wie Todesfälle und Unfälle mit Verletzungsfolgen zu bekämpfen. Angesichts des kontinuierlich ansteigenden Verkehrsaufkommens scheinen Blitzer aus präventivem Blickwinkel eine lohnende Massnahme zum Schutz der öffentlichen Sicherheit zu sein.[109] Die Forscher sagen jedoch auch, dass dieses Fazit

---

103 Zum Ganzen: <https://www.crimesolutions.gov/ProgramDetails.aspx?ID=273>.

104 Steinbach et al., 8.

105 Steinbach et al., 8.

106 Steinbach et al., 7.

107 Steinbach et al., 45.

108 Steinbach et al., 45.

109 Steinbach et al., 3.

mit Vorsicht zu geniessen sei. Die untersuchten Studien zeigen eine grosse Bandbreite an Qualität und Unterschiede im Setting und Zeiträume der Datenkollektion, so dass Vergleiche schwierig sind.[110]

IV. Entwicklungstendenzen

Bekanntermassen ist Kriminalität nicht gleichmässig verteilt über Orte, Personen oder Zeiten. Um effektiv und wirkungsvoll Prävention zu betreiben, müssen präventive Massnahmen dorthin gerichtet werden, wo Kriminalität am stärksten ausgeprägt ist.[111] Anstatt zu versuchen, alle Verbrechen überall zu verhindern, werden die Bemühungen auf diejenigen konzentriert, die den grössten präventiven Nutzen bringen, unabhängig davon, ob sie in Bezug auf ihren Beitrag zur Gesamtkriminalität, ihrer wirtschaftlichen Folgen oder ihre Rolle bei der Förderung von Angst und Unruhe definiert sind. *Hot Spots* ist eines der Konzepte, welches dieses Prinzip anwendet. *Hot Spots*, ein geografisches Konzept, bezieht sich auf Orte oder Gegenden, die eine hohe Quote an gemeldeten Straftaten in einer relativ kurzen Zeit registrierten.[112]

Des Weiteren ist auch bekannt, dass Kriminalität eine Phase der Umstrukturierung unterläuft. Die „traditionelle" Kriminalität ist gemäss offiziellen Statistiken rückläufig und gleichzeitig sind neue Formen der Kriminalität und neue Formen der Ausübung der traditionellen Kriminalität entstanden.[113] Dazu gehören digital begünstigte und bedingte Straftaten in denen das Internet und die sozialen Medien eine verursachende Rolle für das Begehen von Straftaten spielen. Einige dieser neuen digitalen Möglichkeiten zur Begehung von Straftaten ermöglichen es, Schäden in grösserem Umfang und manchmal auch in grosser Entfernung zwischen Tatperson und geschädigte Person durchzuführen, was zu einer stärkeren Trennung zwischen dem Ort der Viktimisierung und dem Wohnsitz des Täters führt als bisher.[114] Dies hat offensichtliche Auswirkungen, nicht nur auf die Herausforderungen der Kriminalprävention, sondern auch auf die technischen Massnahmen, die zur Kriminalprävention konzipiert und verwendet werden.

Um den neuen Herausforderungen gerecht zu werden, wird eine Neuausrichtung der Aspekte der evidenzbasierten Forschung gefordert, welcher mit dem Übergang von „What Works?" zu „What Matters?" am besten verdeutlicht wer-

110 Steinbach et al., 45.

111 Clarke/Webb, 1.

112 Clarke, 1 ff.; Sherman et al., 1 ff.

113 Bundesamt für Statistik BFS, 7.

114 Innes/Robinson/Levi, 1.

den kann. Der Vorschlag ist, die Forschung zu erweitern und dabei zu helfen, die Kriminalitätsprobleme in Bezug auf ihre Prävalenz-, Verteilungs- und Schadensauswirkungen besser zu verstehen und zu kalibrieren, damit potentiell wirksame Interventionsprogramme identifiziert werden können. Anstelle nur zu betonen was funktioniert, wäre es eine Möglichkeit, sich die Frage zu stellen „What Matters?", also „Was spielt eine Rolle?", um die begrenzten Ressourcen auf diejenigen Vorfälle und Probleme auszurichten, die einen besonderen (öffentlichen) Wert haben.[115]

1. Predictive Policing und PRECOBS

Digitale, raumbezogene Prognoseverfahren unterstützen seit einiger Zeit die Arbeit von schweizerischen Polizeikorps und eröffnen dabei neue Chancen für die Kriminalprävention.[116] *Predictive Policing* wird auf Deutsch zuweilen als „vorausschauende Polizeiarbeit" übersetzt und bestimmt gemäss Leese den Diskurs wenn es um technologische Innovationen bei der Verbrechensbekämpfung geht.[117] Mit Predictive Policing werden gemeinhin verschiedene Verfahren gemeint, welche die Wahrscheinlichkeit für das Auftreten von Straftaten prognostizieren. Damit geben sie der Polizei die Gelegenheit, präventive Massnahmen zur Verhinderung der prognostizierten Ereignisse zu ergreifen.[118] Neben Polizeibehörden entwickeln auch kommerzielle Firmen Softwarelösungen, die im Kampf gegen Kriminalität helfen sollen. Neben der Stadtpolizei Zürich arbeiten in der Schweiz verschiedene Kantonspolizeien mit Predictive Policing Software.[119]

Die Stadtpolizei Zürich setzt dabei auf das kommerzielle Software-Paket *PRECOBS* (Pre Crime Observation System).[120] Die Software konzentriert sich auf die Prognose von Einbruchdiebstahlsdelikten. Dies ist gemäss Leese eine verhältnismässig häufig auftretende Straftat, für welche die Polizeibehörden in der Regel über eine gute Datengrundlage hinsichtlich der räumlichen und zeitlichen Verteilung von Einbrüchen sowie deren Tatmerkmalen verfügen. Somit können Prognosemodelle mithilfe weniger Datenpunkte erstellt werden. Der Einsatz von Predictive Policing ist in der Schweiz momentan nur auf einen verhältnismässig kleinen Bereich von präventiver Polizeiarbeit beschränkt.[121]

---

115 Innes/Robinson/Levi, 8.

116 Leese, 57.

117 Leese, 57.

118 Leese, 57.

119 Leese, 57 f.

120 <http://www.ifmpt.de/project_zuerich.html>.

121 Leese, 58.

Gemäss Leese können die zwei Hauptspielarten von Predictive Policing grob anhand der Fragen „Wer?“ und „Wo?“ unterschieden werden. Die Frage „Wer?“ befasst sich damit, wie Personen zu Straftätern oder zu Opfer von Straftaten werden können. Erstere findet sich in Ansätzen, die sich damit befassen, wie Personen zu Straftätern oder zu Opfern von Straftaten werden könnten. Versucht wird, anhand von bestimmten Daten, beispielsweise über den Kontakt von Personen zu errechnen, mit welchem Risiko eine Person eine gewisse Straftat verüben könnte. Wird ein solches Risiko festgestellt, dann kann die Person unter Beobachtung gestellt werden oder auch bspw. Angebote zur Teilnahme an Präventionsprogramme erhalten. Wie erfolgreich solche Angebote sind, ist nicht bekannt.[122] Es ist nicht verwunderlich, dass diese Herangehensweise Kritiker auf den Plan ruft, da durch die erstellten Risikoprofile das Risiko gross ist, dass Vorurteile über gewisse Bevölkerungsgruppen oder Minderheiten wiedergegeben und verstärkt werden. Ein weiterer Kritikpunkt bezieht sich auf die Verarbeitung personenbezogener Daten.[123]

2. Big Data und Artificial Intelligence

In der Gesellschaft wie auch im Bereich der Kriminalprävention nimmt die Bedeutung von Informationstechnologie immer weiter zu. Dabei haben technische Massnahmen zur Kriminalprävention das Potential zur Verbesserung der Effizienz von Wirksamkeit im Strafrechtssystem. Angesichts der zunehmenden Abhängigkeit von Informationstechnologie und deren Massnahmen zur Kriminalprävention ist es überraschend, dass wir nicht mehr über die Wirksamkeit der neuen technischen Massnahmen (im Bereich Software) wissen.[124]

Der routinemässige Einsatz digitaler Geräte in unserem aktuellen Lebensbereich verändert natürlich auch die traditionellen Formen und Organisationsweisen der Polizei und der gesamten Strafverfolgung grundlegend. Wie bereits in diesem Beitrag erwähnt wurde, verändert sich auch in polizeilicher Hinsicht einiges, man denke an das Aufkommen von Risikomanagement Software, Predictive Policing oder das Aufkommen von Überwachungssystemen wie CCTV.[125] Diese Arten der Anwendungen erzeugen neue Formen von Wissen und Fachwissen im Bereich der Bekämpfung von Kriminalität, wie auch deren Prävention.[126]

---

122 Leese, 59.

123 Leese, 59.

124 Byrne/Marx, 24.

125 Smith/Bennett Moses/Chan, 260.

126 Smith/Bennett Moses/Chan, 260.

Big Data sind riesige Datenmengen, die aus hinterlassenen Datenspuren besteht.[127] Auch wenn die Datensammlung anonym vonstattengeht, der Zweck des Ganzen ist die Personalisierung. Personalisierte Daten sind nicht nur für die polizeiliche Arbeit nützlich sein, sondern werden auch in weiteren Bereichen wie dem Detailhandel, angewendet werden.[128]

Aktuelle Entwicklungen wie Big Data- bzw. Predictive Policing verweisen dabei auf eine weitere Entwicklung im Bereich der Kriminalprävention hin. Es handelt sich dabei um den Trend zu sogenannten präemptiven oder vorbeugenden Handlungen, die lediglich auf der Wahrscheinlichkeit basieren, dass etwas passieren könnte. Klassische präventive Massnahmen basieren zumindest auf beobachteten und als riskant eingestuften Verhaltensweisen oder Gegebenheiten, die dann als Indikatoren zukünftiger Abweichungen verstanden werden. Bei vorbeugenden Massnahmen erfolgt ein Eingriff in der Gegenwart bereits wenn nicht ausgeschlossen werden kann, dass in naher oder ferner Zukunft etwas Unerwünschtes wie Kriminalität erfolgen könnte.[129]

Schlussendlich stellt sich die Frage, ob es ein Gewinn für uns und unsere Gesellschaft ist, wenn wir auf technische Massnahmen zur Kriminalprävention setzen, oder ob wir dabei auch verlieren können. Technische Massnahmen können neben intendierten auch nicht-intendierte und damit nicht geplante Folgen haben. Eine mögliche wäre, dass im Laufe der Zeit Polizisten, Richter (wenn Algorithmen Urteile fällen) und viele andere Personen im Justizbereich ersetzt werden. Vielleicht wird irgendwann die Frage gestellt, warum es Polizisten braucht, die auf Strassen patrouillieren, wenn über die technischen Ressourcen verfügt wird, wie Kameras zur Erkennung von Geschwindigkeitsübertretungen oder Rotlichtverletzungen, Videoüberwachung öffentlicher Plätze und es genügt, wenn eine kleine Anzahl von Polizisten aus der Ferne die Situation überwachen?

Nicht nur die Folgen des Einsatzes technischer Massnahmen sind zu beachten, ein Augenmerk ist auch auf die zunehmende Abhängigkeit von privaten Firmen zu richten. Wie viele von uns können die aktuell verwendeten technischen Massnahmen bis ins Detail verstehen und anwenden? Wer hat noch die notwendigen technologiebasierten Fähigkeiten, um mit den neusten technischen Massnahmen umgehen zu können? Wir sind gezwungen, heute mehr als je zuvor in unserer Geschichte, uns auf den Privatsektor zu verlassen im Bereich der technischen Massnahmen und generell im Informationsmanagement. Dies wird ungeahnte Folgen haben.

---

127 Legnaro/Kretschmann, 105.

128 Legnaro/Kretschmann, 106.

129 Lampe, 183 f.

Literaturverzeichnis

Bowers K./Guerette R., Effectiveness of Situational Crime Prevention, in: Bruinsma/Weisburd, Encyclopedia of Criminology and Criminal Justice, New York 2014, 1318-1329.

Bundesamt für Statistik BFS, Polizeiliche Kriminalstatistik (PKS), Jahresbericht 2019 der polizeilich registrierten Straftaten, Neuchâtel 2019.

Byrne James M./Marx Gary, Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact, Cahiers Politiestudies 2011, 3, 17-40.

Choi K.S./Librett Mitch/Collins TJ, An empirical evaluation: gunshot detection system and its effectiveness on police practices, Police Practice and Research 2014, 1, 48-61.

Clarke Ronald, Situational crime prevention, 2. ed., Guilderland/Monsey/New York 1997.

Clarke Ronald/Webb Barry, Hot Products: understanding, anticipating and reducing demand for stolen goods, London 1999.

De Waard Jaap, What Works?: A systematic overview of recently published meta evaluations/synthesis studies within the knowledge domains of Situational Crime Prevention, Policing, and Criminal Justice Interventions, 1997-2018.

Dollinger Bernd, Die Konstruktion on Evidenz in der Präventionsarbeit, in: Walsh et al., Evidenzorientierte Kriminalprävention in Deutschland, Wiesbaden 2018, 187-204.

Fagan Abigail Fagan/Buchanan Molly, What Works in Crime Prevention?, Criminology & Public Policy 2016, 3, 617-649.

Farrington David P./Gill Marin/Wapples Sam J./Argomaniz Javier, The effects of closed-circuit television on crime: meta-analysis of an English national quasi-experimental multi-site evaluation, Journal of Experimental Criminology 2007, 1, 21-38.

Feltes Thomas, Wirksamkeit technischer Einbruchsprävention bei Wohn- und Geschäftsobjekten, Bachum 2004.

Hummer ByDon/Byrne James, Technology, innovation, and twenty-first-century policing, in: McGuire/Holt, The Routledge Handbook of Technology, Crime and Justice, London 2017, 375-389.

Innes Martin/Robinson Amanda/Levi Michael, Preventing Future Crimes & Crime Prevention Futures, Cardiff 2018.

Kaiser Günther, Kriminologie, 10., völlig neubearb. Aufl., Heidelberg 1997.

Kett-Straub Gabriele, Dient die Technoprävention der Vermeidung von Kriminalität? – Insbesondere die Wirksamkeit der staatlichen Videoüberwachung im öffentlichen Raum, Zeitschrift für die gesamte Strafrechtswissenschaft 2011, 1, 110-133.

Koper Christopher S./Lum Cynthia/Willis James J./Woods Daniel/Hibdon Julie, Realizing the Potential of Technology in Policing, Fairfax, VA 2015.

Kunz/Singelnstein, Kriminologie, 7., grundlegend überarb. Aufl., Bern 2016.

Kury H., Präventionskonzepte, in: Lange/Ohly/Reichertz, Auf der Suche nach neuer Sicherheit, Wiesbaden 2009, 21-48.

Lampe Dirk, Prävention. Praktiken, Kritiken und Leerstellen, Kriminologisches Journal 2018, 3, 178-187.

Leese Matthias, Predictive Policing in der Schweiz: Chancen, Herausforderungen, Risiken, in: Nünlist/Thränert, Bulletin 2018 zur schweizerischen Sicherheitspolitik, Zürich 2018, 57-71.

Legnaro Aldo/Kretschmann Andrea, Das Polizieren der Zukunft, Kriminologisches Journal 2015, 2, 94-111.

Maass Harald, Die Hölle, Das Magazin 12, 23. März 2019, 8-17.

Piza Eric L./Welsh Brandon C./Frarrington David P./Thomas Amanda L., CCTV surveillance for crime prevention, Criminology & Public Policy 2019, 1, 135-159.

Sherman Lawrence W./Gottfredson Denise C./MacKenzie Doris L./Eck John/Reuter Peter/Bushway Shawn D., Preventing Crime: What Works, What Doesn't, What's Promising, Maryland 1998.

Sidebottom Aiden/Thornton Amy/Tompson Lisa/Belur Jyoti/Tilley Nick/Bowers Kate, A Systematic Review of Tagging as a Method to Reduce Theft in Retail Environments, London 2017 (zit. Sidebottom et al., A Systematic Review).

Sidebottom Aiden/Thomposon Lisa/Thornton Amy/Bullock Karen/Tilley Nick/Bowers Kate/Johnoson Shane D., Gating Alleys to Reduce Crime: A Meta-Analysis and Realist Synthesis, London 2017 (zit. Sidebottom et al., Gating Alleys to Reduce Crime).

Smith Gavin J.D./Bennett Moses Lyria/Chan Janet, The Challenges of Doing Criminology in the Big Data Era, The British Journal of Criminology 2017, 2, 259-274.

Smith Finley Joanne, Securitization, insecurity and conflict in contemporary Xinjiang: has PRC counter-terrorism evolved into state terror?, Central Asian Survey 2019, 1, 1-26.

Steinbach Rebecca/Perkins Chloe/Edwards Phil/Beecher Deirdre/Roberts Ian, Speed Cameras to Reduce Speeding Traffic and Road Traffic Injuries, London 2016.

Tilley Nick/Sidebottom Aiden, Situational Crime Prevention, in: Bruinsma/Weisburd, Encyclopedia of Criminology and Criminal Justice, New York 2014, 4864-4882.

Tseloni Andromachi/Thompson Rebecca/Tilley Nick, Reducing Burglary, Cham 2018.

Welsh Brandon C./Farrington David P., Crime prevention effects of closed circuit television: a systematic review, London 2002 (zit. Welsh/Farrington, Crime prevention effects).

Welsh Brandon C./Farrington David P., Effects of Closed Circuit Television Surveillance on Crime, London 2008 (zit. Welsh/Farrington, Effects of Closed Circuit Television).

Welsh Brandon C./Farrington David P., Effects of Improved Street Lighting on Crime, Lowell 2008 (zit. Welsh/Farrington, Effects of Improved Street Lighting).

Welsh Brandon C./Farrington David P., Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis, Justice Quarterly 2009d, 4, 716-745 (zit. Welsh/Farrington, Public Area CCTV and Crime Prevention).

Der Einsatz von Electronic Monitoring in der Schweiz - Ein Überblick

Jasmine Stössel*

Inhalt

* Der vorliegende Text basiert zu wesentlichen Teilen auf der Dissertation der Autorin zum Electronic Monitoring, vgl. Stössel Jasmine, Electronic Monitoring im Schweizer Erwachsenenstrafrecht – unter besonderer Berücksichtigung der Änderungen des Sanktionenrechts, Zürich 2018, unter Beizug neuer Literatur und Rechtsprechung zum Thema.

I. Einleitung

Die elektronische Überwachung, auch Electronic Monitoring oder kurz EM genannt, bietet seit den ersten Erfahrungen im schweizerischen Kontext in Form des interkantonalen Modellversuchs von 1999-2002 – trotz der durchwegs positiven Ergebnisse desselben – Diskussionsstoff, indem insbesondere im öffentlichen Diskurs bis heute eine enorme Skepsis spürbar ist. So wird etwa behauptet, dass Electronic Monitoring keinen oder nur einen minimalen Strafcharakter aufweise oder sich Probleme in Bezug auf Sicherheitsaspekte ergeben würden. Seit dem 1. Januar 2018 ist Electronic Monitoring als Vollzugsform für kurze Freiheitsstrafen sowie als Vollzugsstufe am Ende längerer Freiheitsstrafen nun in Art. 79b des Schweizerischen Strafgesetzbuches gesetzlich verankert und damit gesamtschweizerisch anzuwenden. Daneben bestehen jedoch noch diverse weitere Anwendungsmöglichkeiten der elektronischen Überwachung, so etwa als Kontrollinstrument strafprozessualer Ersatzmassnahmen oder zivilrechtlicher Gewaltschutzmassnahmen. Der vorliegende Beitrag soll deshalb anhand einer Darstellung der Electronic Monitoring zugrunde liegenden Überwachungstechnologien, ausgewählter Anwendungsfelder im schweizerischen Kontext sowie dazugehöriger spezialpräventiver Aspekte das Verständnis der elektronischen Überwachung – insbesondere auch im Bereich eines präventiven Einsatzes – fördern und die jeweiligen Ausgestaltungen kritisch hinterfragen.

II. Überwachungstechnologie

Um die Möglichkeiten und Grenzen von Electronic Monitoring bestimmen zu können, ist das Verständnis der verschiedenen Überwachungstechnologien zentral. Die Überwachungsarten von Electronic Monitoring lassen sich dabei grob in Überwachungssysteme der ersten Generation, welche sich auf die Kontrolle der An- oder Abwesenheit einer Person an einem bestimmten Ort beschränken, sowie in Überwachungssysteme der zweiten Generation, womit der aktuelle Aufenthaltsort der überwachten Person bestimmt werden kann, gliedern.

1. Anwesenheitskontrolle

Beim auf der Radiofrequenz-Technologie basierenden System der Anwesenheitskontrolle wird vom Sender, welcher der Überwachte permanent tragen muss, ein Signal an ein in der Wohnung des Überwachten stationiertes Empfangsgerät abgegeben. Über das Telefon- oder Mobilfunknetz wird das Signal an die Überwachungszentrale bzw. die zuständige Stelle weitergeleitet, wo die eingegangenen Daten mit den programmierten Daten[1] des Überwachten verglichen werden.[2] Korrespondiert die Abwesenheit nicht mit einer festgelegten Zeit, während der die überwachte Person die Wohnung verlassen darf, z.B. für Arztbesuche, oder verlassen muss, z.B. zur Arbeit, wird ein Alarm ausgelöst.[3] Um ein Entfernen oder andere Manipulationen am vom Überwachten zu tragenden Sender zu verhindern, findet sich im Plastikband oft ein eingebauter Stromkreis, welcher bei Durchtrennung ebenfalls das Auslösen eines Alarms zur Folge hat.[4] Mit dem Radiofrequenz-System lässt sich somit nur feststellen, ob der Überwachte an einem bestimmten Ort – meist in dessen Wohnung – an- oder abwesend ist, d.h. ob er sich in Reichweite des Empfangsgeräts befindet, wobei der konkrete Aufenthaltsort bei nicht erfolgter Rückkehr nach Hause nicht ermittelt werden kann.[5]

2. Aufenthaltskontrolle

Die Aufenthaltskontrolle mittels GPS-Technologie ermöglicht eine kontinuierliche Aufenthaltskontrolle und die Erstellung von Bewegungsprofilen.[6] Technisch existieren sog. One Piece Tracking- und Two Piece Tracking-Systeme: Während beim One Piece Tracking nur ein einteiliges Gerät erforderlich ist, welches über das Mobilfunknetz kommuniziert, erfordert das Two Piece Tracking zwei Geräte, einen Sender sowie einen Tracker mit GPS-Empfänger, wobei der Sender dem herkömmlichen Sender entspricht, wie er bei der Radiofrequenz-Technologie verwendet wird.[7] Bei der Aufenthaltskontrolle mittels GPS-Technologie können die Bewegungen der überwachten Person

---

1 So wird etwa im Rahmen von Art. 79b StGB mit dem Überwachten ein individueller Wochenplan, welcher u.a. die An- und Abwesenheitszeiten in der Wohnung zum Inhalt hat, festgelegt, vgl. dazu unten, III.2.a)iv.

2 Vgl. etwa SCHLÜSSELBERGER, 76 ff.; WEBER, 21; WERNINGER, 217.

3 AEBERSOLD, 368; BAECHTOLD/WEBER/HOSTETTLER, II.5. Rz 70; HOCHMAYR, 537; Konkordat Nordwest- und Innerschweiz, Grundlagenpapier EM, 1 f.

4 SCHLÜSSELBERGER, 78; WEBER, 21.

5 BERLOVAN, N 11; SCHLÜSSELBERGER, 82; WEBER, 23.

6 BERLOVAN, N 16; SCHLÜSSELBERGER, 83; WEBER, 30 f.

7 Vgl. dazu ausführlich SCHLÜSSELBERGER, 79.

entweder retrospektiv oder in Echtzeit verfolgt werden. Beim retrospektiven Tracking, auch *passive GPS-Überwachung* genannt, werden die Bewegungsdaten des Überwachten während des Tages aufgezeichnet und in bestimmten Zeitintervallen
– z.B. alle 24 Stunden – von der zuständigen Behörde überprüft.[8] Beim Real-Time Tracking, auch *aktive GPS-Überwachung* genannt, besteht die Möglichkeit ständiger Lokalisierung und sofortigen Eingreifens, weshalb nach Eingang einer Alarmmeldung bei der zuständigen Stelle umgehend eine vordefinierte Intervention ausgelöst werden kann.[9] Diese vordefinierte Reaktion auf einen Verstoss kann aus einer telefonischen Kontaktaufnahme mit dem Überwachten bis hin zu einer Einleitung von polizeilichen Interventionen[10] bestehen.[11] Eine Kombination zwischen aktiver und passiver GPS-Überwachung stellt das Hybridsystem dar, indem die Bewegungen des Überwachten aufgezeichnet und, falls vorher festgelegte Überwachungsparameter verletzt werden, in den Modus der Echtzeitverfolgung gewechselt wird.[12] Gemäss Zwischenbericht der KKJPD wird im schweizerischen Kontext erwartet, dass in den nächsten Jahren hauptsächlich die passive GPS-Überwachung zur Anwendung kommen wird.[13]

Bei einer Überwachung mit GPS können sog. *Inklusions- und Exklusionszonen* festgelegt werden, in denen sich der Überwachte aufhalten muss bzw. die er nicht betreten darf, wobei bei einem Verstoss gegen einen solchen Rayonarrest bzw. ein Rayonverbot eine entsprechende Meldung ausgelöst wird.[14] Exklusionszonen können etwa um das Umfeld – z.B. den Wohn- und Arbeitsort – eines Opfers von häuslicher Gewalt, Stalking etc. konstruiert werden.[15] In diesem Zusammenhang kann die Errichtung einer sog. *Pufferzone* sinnvoll sein, womit Areale ausserhalb und angrenzend an eine Exklusionszone definiert werden, deren Betreten bereits einen vorzeitigen Alarm auslöst, um

---

8 Vgl. etwa BSK StGB-Koller, Art. 79b N 25; SCHLÜSSELBERGER, 84.

9 BSK StGB-Koller, Art. 79b N 25; SCHLÜSSELBERGER, 84.

10 Diese Überwachungsart, womit die Verhinderung einer Flucht oder Tat angestrebt wird, wird teilweise als *aktiv PLUS-Überwachung* bezeichnet, vgl. KKJPD, Zwischenbericht EM, 6.

11 SCHLÜSSELBERGER, 84, wobei dieser zutreffend darauf hinweist, dass es für eine erfolgversprechende Polizeiintervention der genauen Bestimmung des Aufenthaltsortes bedarf, was unter Umständen nicht zu 100% gewährleistet werden kann, sowie die effektive Reaktionszeit der Polizei je nach Uhrzeit und Arbeitsvolumen stark variiert.

12 Vgl. dazu STÖSSEL, 51 m.w.N.

13 KKJPD, Zwischenbericht EM, 6.

14 BERLOVAN, N 17; Konkordat Nordwest- und Innerschweiz, Grundlagenpapier EM, 2; SCHLÜSSELBERGER, 86.

15 Vgl. anstelle vieler WENNERBERG, 125.

genügend Zeit für die Ergreifung entsprechender Massnahmen zu haben.[16] Darüber hinaus besteht auch die Möglichkeit der Festlegung sog. *dynamischer Rayons*, d.h. das Opfer wird ebenfalls mit einem GPS-Sender ausgestattet, welchen es ständig bei sich zu tragen hat, wodurch eine mobile Exklusionszone festgelegt werden kann.[17]

Im schweizerischen Kontext wird zurzeit die EM-Technik von zwei Herstellern eingesetzt, wobei 21 Kantone an der Übergangslösung des Kantons Zürich angeschlossen sind und fünf Kantone die Technik von GEOSATIS, einem schweizerischen Hersteller von End-to-End-Lösungen für die elektronische Überwachung, nutzen.[18] Die definitive nationale Lösung soll per 2023 in Betrieb genommen werden, wobei schweizweit eine einzige Technik und eine (dreisprachige) Überwachungszentrale mit einem zentralen Server im Kanton Jura eingerichtet werden soll.[19] Zudem wird die Einrichtung einer gemeinsamen interkantonalen Trägerschaft für die Investition und den Betrieb des Gesamtsystems Electronic Monitoring in Form eines Vereins beabsichtigt.[20]

3. Technische Grenzen

Während die technische Grenze des Radiofrequenz-Systems augenscheinlich darin liegt, dass der Aufenthaltsort des Überwachten bei einer unerlaubten Entfernung nicht feststellbar ist, bleibt zu betonen, dass selbst durch GPS-gestütztes Electronic Monitoring zwar der Standort des Überwachten ermittelt, jedoch weder das unbefugte Verlassen der Wohnung noch das Betreten einer Exklusionszone verhindert werden kann. Möglich ist lediglich die Feststellung von Verstössen, um diese den zuständigen Stellen zur Kenntnis zu bringen und – falls notwendig – ein zeitnahes Eingreifen einzuleiten.[21] Andererseits bestehen aber auch Grenzen, welche sich aus der GPS-Technologie selbst ergeben: So ist etwa der Satellitenempfang an bestimmten Orten eingeschränkt, z.B. innerhalb von Gebäuden, in Kellern oder Tunnels.[22] Diesem Problem kann mit einer kombinierten Anwendung von GPS- und Radiofrequenzsystemen, indem eine Person während der Nacht zu Hause mittels Radiofre quenz-System und am Tag, wenn das Haus verlassen wird, mittels

16 Vgl. etwa Scottish Government, 17.

17 SCHLÜSSELBERGER, 86; WENNERBERG, 125. Diese Art der elektronischen Überwachung wird in der Literatur auch als *bilaterales Electronic Monitoring* bezeichnet.

18 KKJPD, Zwischenbericht EM, 6; BSK StGB-Koller, Art. 79b N 8.

19 KKJPD, Zwischenbericht EM, 5; BSK StGB-Koller, Art. 79b N 8.

20 KKJPD, Zwischenbericht EM, 5; BSK StGB-Koller, Art. 79b N 8.

21 Vgl. auch SCHLÜSSELBERGER, 86; WEBER, 41.

22 Anstelle vieler FERREIRA BROQUET, N 63; SCHLÜSSELBERGER, 86 f.

GPS überwacht wird, entgegengewirkt werden.[23] An Orten, welche für GPS-Signale unzulänglich sind, kann das Mobilfunknetz dazu dienen, den jeweiligen Aufenthaltsort über die Distanz zum nächsten Mobilfunkmast zu berechnen.[24] Dabei variiert die Genauigkeit der Ortung je nach Deckungsgrad der Gegend mit Mobilfunkmasten.[25] Eine weitere Ortungsmöglichkeit besteht über das WLAN, indem verschiedene WLAN-Netzwerke in Reichweite wahrgenommen werden und eine Lokalisierung mithilfe des Prinzips der Triangulation erfolgt.[26] Eine Ortung über das Mobilfunknetz oder mittels WLAN ist jedoch nicht annähernd so genau und zuverlässig wie mittels GPS.[27]

III. Anwendung in der Schweiz

1. Überblick Anwendungsbereiche

Die Möglichkeiten für die Anwendung von Electronic Monitoring sind äusserst vielseitig. Im Zentrum steht der Einsatz von Electronic Monitoring im Strafvollzug in Form eines Ersatzes kurzer Freiheitsstrafen (Front Door-Variante) oder am Ende längerer Freiheitsstrafen als neu konzipierte Vollzugslockerungsstufe (Back Door-Variante). Ebenfalls kann Electronic Monitoring zur zusätzlichen Überwachung von Vollzugslockerungen[28] eingesetzt werden, wobei für die Schaffung einer expliziten gesetzlichen Grundlage die Kantone zuständig sind, zumal es sich dabei um Strafvollzugsrecht im engeren Sinn handelt. Des Weiteren besteht die Möglichkeit einer Anwendung von Electronic Monitoring im Strafprozessrecht als Kontrollinstrument von Ersatzmassnahmen, zur Überwachung eines strafrechtlichen Kontakt- und Rayonverbotes nach Art. 67b Abs. 3 StGB[29] sowie zur Überprüfung eines zivilrechtlich angeordneten Annäherungs-, Orts- oder Kontaktverbots i.S.v. Art. 28b ZGB. In der Folge wird der Einsatz von Electronic Monitoring im Rahmen von Art. 79b StGB (Front Door- und Back Door-Variante), im Strafprozessrecht sowie im Zusammenhang mit zivilrechtlichen Schutzmassnahmen exemplarisch dargestellt, um die Unterschiede zwischen den einzelnen Anwendungsmöglichkeiten aufzuzeigen.

---

23 Scottish Government, 17 f.

24 Scottish Government, 15; vgl. auch SCHLÜSSELBERGER, 86 f.

25 SCHLÜSSELBERGER, 87.

26 BROWN/MCCABE/WELLFORD, 4-9.

27 Vgl. STÖSSEL, 53 ff. m.w.N.

28 Dazu ausführlich STÖSSEL, 232 ff.

29 Dazu ausführlich STÖSSEL, 259 ff.

	Regelung	Ziel	Bevorzugte Überwachungstechnik	Individuelle Vollzugsplanung
Front Door	Art. 79b Abs. 1 lit. a StGB	Ersatz kurzer Freiheitsstrafen	Radiofrequenz	Ja
Back Door	Art. 79b. Abs. 1 lit. b StGB	Vollzugsstufe am Ende langer Freiheitsstrafen	Radiofrequenz	Ja
Überwachung von Vollzugslockerungen	kantonales Recht; Art. 74/75 StGB	zusätzliche Sicherheitsmassnahme	GPS	Nein
Kontrolle von strafprozessualen Ersatzmassnahmen	Art. 237 Abs. 3 StPO	Kontrolle von Ersatzmassnahmen, insbesondere Ein- und Ausgrenzungen nach Art. 237 Abs. 2 lit. c StPO	GPS	Nein
strafrechtliches Kontakt- und Rayonverbot	Art. 67b Abs. 3 StGB	Überprüfung von strafrechtlichen Kontakt- und Rayonverboten	GPS	Nein
zivilrechtliche Schutzmassnahmen bei häuslicher Gewalt	Art. 28c E-ZGB	Überprüfung von zivilgerichtlich angeordneten Annäherungs-, Orts- oder Kontraktverboten i.S.v. Art. 28b ZGB	GPS	Nein

Überblick über die Anwendungsbereiche von EM in der Schweiz

2. Darstellung ausgewählter Anwendungsbereiche

a) Electronic Monitoring im Strafvollzug

aa) Vom interkantonalen Modellversuch 1999-2002 zu Art. 79b StGB

Die älteste Variante von Electronic Monitoring in der Schweiz bildet dessen Einsatz im Strafvollzug als Ersatz kurzer Freiheitsstrafen oder am Ende längerer Freiheitsstrafen im Anschluss oder anstelle des Arbeitsexternats. Im April 1999 erhielten die Kantone Basel-Stadt, Basel-Landschaft und Bern (Teilprojekt Deutschschweiz) sowie Waadt, Tessin und Genf (Teilprojekt Romandie) auf entsprechende Gesuche hin eine Bewilligung zur Teilnahme an einem Pilotprojekt mit Electronic Monitoring für die Dauer von drei Jahren.[30] Die Aus-

[30] Beschluss BR 2000, 3502; Berlovan, N 20; ausführlich Weber, 165. Für eine Übersicht über die während des Modellversuchs sowie bis zum Inkrafttreten von Art. 79b StGB geltenden gesetzlichen Grundlagen in Form der von den beteiligten Kantonen erlassenen Verordnungen betreffend Electronic Monitoring vgl. Stössel, 89 f. sowie 115.

wertung des Modellversuchs 1999-2002 ergab äusserst positive Ergebnisse, indem sich Electronic Monitoring als sozialverträglichste Vollzugsform des schweizerischen Strafvollzugssystems erwies, wobei von den involvierten Personen insbesondere die Betreuung während des Vollzugs als zentrales Element wahrgenommen wurde.[31] Insbesondere die Vernetzung mit langfristig verfügbaren Hilfsangeboten erwies sich als wichtig, um den individuellen Problemfeldern der Teilnehmer zu begegnen, wobei durch die Betreuung vor Ort zudem ein umfassender Einblick in die Lebensumstände und Problemfelder der Teilnehmer ermöglicht wurde, was eine ideale Intervention erlaubte.[32] Die Bewilligung des Bundesrates wurde schliesslich mehrmals verlängert und im Jahr 2003 auf den Kanton Solothurn ausgedehnt, wobei eine letzte Verlängerung am 2. September 2015 bis zum Inkrafttreten von Art. 79b StGB am 1. Januar 2018 erfolgte.[33]

bb) Front Door-Variante (Art. 79b Abs. 1 lit. a StGB)

Die Front Door-Variante wird in Art. 79b Abs. 1 lit. a StGB geregelt, wonach die Vollzugsbehörde auf Gesuch des Verurteilten hin den Einsatz elektronischer Geräte und deren feste Verbindung mit dem Körper des Verurteilten für den Vollzug einer Freiheitsstrafe oder einer Ersatzfreiheitsstrafe von 20 Tagen bis zu zwölf Monaten anordnen kann.[34] Mit dem Einsatz von Electronic Monitoring als Ersatz kurzer Freiheitsstrafen wird die desintegrative Wirkung eines stationären Freiheitsentzuges[35] vermieden, sodass der Verurteilte in seinem sozialen Umfeld verbleiben und seine Arbeitsstelle fortführen kann, womit für eine spätere Wiedereingliederung wichtige Faktoren aufrechterhalten werden.[36] Es ist jedoch zu beachten, dass Electronic Monitoring insbesondere eine Alternative zur Halbgefangenschaft und weniger zum Normalvollzug darstellt – dies einerseits aufgrund des Strafbereichs der beiden alternativen Vollzugs-

---

31 e&e, Schlussbericht, 91.

32 e&e, Schlussbericht, 98; Dies., Rückfalluntersuchung, 37.

33 Beschluss BR 2015, 6925 f.; vgl. auch BSK StGB-Koller, Art. 79b N 3; Werninger, 215. Für einen tabellarischen Überblick über die Vollzugsmodalitäten während des Modellversuchs sowie bis zum Inkrafttreten von Art. 79b StGB vgl. Stössel, 102 f. sowie 150 ff.

34 Bei teilbedingten Freiheitsstrafen ist gemäss bundesgerichtlicher Rechtsprechung die ausgesprochene Strafe *ab initio* massgebend (Urteil des BGer 6B_1253/2015 vom 17. März 2016, E. 2.6), was zur Folge hat, dass der Vollzug mit Electronic Monitoring nur dann möglich ist, wenn die Gesamtstrafe nicht mehr als 12 Monate beträgt. Ausführlich zu dieser Problematik sowie zum Vollzug von Reststrafen nach Anrechnung der Untersuchungshaft Stössel, 182 ff.

35 Dass mit kurzen Freiheitsstrafen regelmässig desozialisierende oder kriminalitätsfördernde Folgen verbunden sind, ist in der Literatur weitgehend unbestritten, vgl. statt vieler Baechtold/Weber/Hostettler, I.4 Rz 5; BSK StGB-Mazzucchelli, Art. 41 N 7 m.w.N.

36 Vgl. Stössel, 370; ebenso BSK StGB-Koller, Art. 79b N 5; Werninger, 218 m.w.N.

formen, andererseits aufgrund der ähnlichen Anordnungsvoraussetzungen.[37] Aber auch im Vergleich mit der Halbgefangenschaft zeigt sich, dass Electronic Monitoring nicht nur desintegrierende Konsequenzen im Bereich der Arbeitswelt, sondern auch im engeren sozialen Netz zu verhindern vermag, wobei gerade die Stabilisierung des sozialen Umfelds für die Legalbewährung nach der Entlassung von ausserordentlicher Wichtigkeit ist.[38]

cc) Back Door-Variante (Art. 79b Abs. 1 lit. b StGB)

Gemäss Art. 79b Abs. 1 lit. b StGB kann die Vollzugsbehörde den Einsatz von Electronic Monitoring anstelle des Arbeitsexternats oder des Arbeits- und Wohnexternats für die Dauer von 3 bis 12 Monaten anordnen. Dabei handelt es sich um eine zusätzliche Vollzugsstufe vor der bedingten Entlassung.[39] Electronic Monitoring im Back Door-Bereich kann damit zu einem individuell begleiteten Übergang in die Freiheit nach längeren Freiheitsstrafen beitragen. Wird Electronic Monitoring anstelle des Arbeitsexternats angeordnet, bedeutet dies, dass dem Gefangenen gestattet wird, auch die Ruhe- und Freizeit ausserhalb der Anstalt zu verbringen, jedoch mit elektronischer Überwachung.[40] Faktisch entspricht dies einem elektronisch überwachten Wohn- und Arbeitsexternat, weshalb mit der Formulierung von Art. 79b Abs. 1 lit. b StGB offenbar die Möglichkeit zur insbesondere zeitlichen Differenzierung geschaffen werden sollte.[41] Damit werden wie bis anhin zwischen (offenem) Normalvollzug und bedingter Entlassung i.d.R. maximal zwei Progressionsstufen zu absolvieren sein, indem der Vollzug mit elektronischer Überwachung entweder *ohne* (allenfalls gefolgt von einem Wohn- und Arbeitsexternat ohne Überwachung) oder *mit* „herkömmlichem" Arbeitsexternat als Einstiegsphase erfolgt.[42] Im ersten Fall handelt es sich um Electronic Monitoring anstelle des Arbeitsexternats, im zweiten Fall um Electronic Monitoring anstelle des Wohn- und Arbeitsexternats. Ob es sinnvoll ist, noch ein gewöhnliches Wohn- und

---

37 Vgl. etwa BSK StGB-KOLLER, Art. 79b N 6 und Art. 77b N 2 f.; WERNINGER, 219. Ausführlich zum Verdrängungseffekt von Electronic Monitoring in Bezug auf die Halbgefangenschaft und den Normalvollzug STÖSSEL, 428 ff.

38 BAECHTOLD/WEBER/HOSTETTLER, II.5 Rz 7 und 67; BSK StGB-KOLLER, Art. 79b N 5; vgl. auch e&e, Schlussbericht, 33 und 97 f.

39 BSK StGB-KOLLER, Art. 79b N 10; vgl. auch BSK StGB-BRÄGGER, Art. 77a N 16.

40 BSK StGB-KOLLER, Art. 79b N 10; vgl. auch BSK StGB-BRÄGGER, Art. 77a N 16; Vollzugslexikon-DERS., 47.

41 BSK StGB-KOLLER, Art. 79b N 10.

42 BSK StGB-KOLLER, Art. 79b N 10; a.A. BSK StGB-BRÄGGER, Art. 77a N 18, welcher es als sinnvoll betrachtet, Electronic Monitoring in aller Regel zwischen den Vollzugsstufen des Arbeitsexternats und des Wohn- und Arbeitsexternats anzuwenden.

Arbeitsexternat nachfolgen zu lassen, ist je nach Einzelfall und Straflänge zu entscheiden. Auch bei der Back Door-Variante ergibt sich kein Verdrängungseffekt in Bezug auf den Normalvollzug, sondern nur bezüglich des Arbeitsexternats; eine reale Verkürzung der Inhaftierungsdauer könnte lediglich dann erzielt werden, wenn das Arbeitsexternat früher ausgesprochen würde.[43]

Gemäss der Statistik des BFS erfolgten im Jahr 2016 von insgesamt 271 Antritten eines Vollzugs mit Electronic Monitoring lediglich 30 im Back Door-Bereich, im Jahr 2017 von insgesamt 235 Antritten 25 im Back Door-Bereich.[44] Damit wird deutlich, dass der Hauptanwendungsbereich von Electronic Monitoring die Front Door-Variante betrifft.

dd) Gemeinsame Voraussetzungen (Art. 79b Abs. 2 StGB)

Die Anordnung von Electronic Monitoring erfolgt auf Gesuch des Verurteilten. Zudem wird vorausgesetzt, dass keine Flucht- oder Rückfallgefahr vorliegt (Abs. 2 lit. a), der Verurteilte über eine dauerhafte Unterkunft (Abs. 2 lit. b) sowie eine geregelte Arbeit, Ausbildung oder Beschäftigung (Abs. 2 lit. c) verfügt. Des Weiteren ist die Zustimmung der in derselben Wohnung lebenden Personen (Abs. 2 lit. d) und die Zustimmung des Verurteilten zum individuellen Vollzugsplan (Abs. 2 lit. e) erforderlich.[45] Der Verurteilte hat sich überdies gemäss Art. 380 Abs. 2 lit. c StGB in angemessener Weise an den Kosten des Vollzugs der elektronischen Überwachung zu beteiligen.[46] Ob die entsprechenden Voraussetzungen vorliegen, wird in einer Eignungsabklärung (sog. *Screening*) geprüft, wobei gestützt auf diese Eignungsabklärung anschliessend die für die Bewilligung zuständige kantonale Behörde über die Zulassung zum Vollzug entscheidet.

---

43 Vgl. dazu ausführlich Stössel, 444 ff. m.w.N.; ebenso BERLOVAN, N 60.

44 BFS, Electronic Monitoring. Für einen detaillierten Überblick über die zahlenmässige Entwicklung von Electronic Monitoring seit dem Jahr 2007 vgl. STÖSSEL, 418 ff.

45 Ausführlich zu den persönlichen Voraussetzungen nach Art. 79b Abs. 2 StGB BSK StGB-KOLLER, Art. 79b N 17 ff., STÖSSEL, 193 ff. sowie WERNINGER, 227 ff. jeweils m.w.N.

46 Bereits nach den bisherigen kantonalen Regelungen wurde vom Verurteilten ein Kostenbeitrag von je nach Kanton zwischen CHF 10.– und CHF 25.– verlangt, wobei dieser bei Vorliegen prekärer finanzieller Verhältnisse auch erlassen werden konnte, vgl. dazu der tabellarische Überblick in STÖSSEL, 150 ff. Die aktuelle Kostenbeteiligung beträgt im Ostschweizer Strafvollzugskonkordat CHF 20.–sowie im Strafvollzugskonkordat Nordwest- und Innerschweiz zwischen CHF 20.– und CHF 40.–, vgl. dazu BSK StGB-KOLLER, Art. 79b N 26 m.w.N.

ee) Abbruch des Vollzugs oder Einschränkung der freien Zeit (Art. 79b Abs. 3 StGB)

Bei Wegfall der Voraussetzungen der fehlenden Flucht- und Rückfallgefahr, der dauerhaften Unterkunft sowie der geregelten Arbeit, Ausbildung oder Beschäftigung von mindestens 20 Stunden pro Woche ist der Vollzug mit Electronic Monitoring gemäss Art. 79b Abs. 3 StGB abzubrechen.[47] Obwohl in Art. 79b Abs. 3 StGB nicht explizit erwähnt, muss der Abbruch des Vollzugs mit Electronic Monitoring auch bei einem Widerruf der Zustimmung der mit dem Verurteilten in derselben Wohnung lebenden Person erfolgen. Eine Fortführung des Vollzugs gegen den Willen der in derselben Wohnung lebenden Person ist jedenfalls undenkbar.[48]

Verletzt der Verurteilte seine im Vollzugsplan festgelegten Pflichten, kann nach dem Wortlaut von Art. 79b Abs. 3 StGB als Konsequenz ein Abbruch des Vollzugs oder alternativ eine Einschränkung der freien Zeit erfolgen. Von den Kantonen ist eine konkretisierende Regelung zu fordern, welche zwischen verschiedenen Schweregraden von Verstössen unterscheidet und die entsprechenden Rechtsfolgen definiert, wie sich dies bereits in der bisherigen Praxis vor Inkrafttreten von Art. 79b StGB bewährt hat.[49] So könnte etwa zwischen leichten Verstössen, die eine schriftliche Verwarnung[50] zur Folge haben, groben Verstössen, welche eine Verkürzung der freien Zeit nach sich ziehen, sowie schweren Verstössen, welche zum Abbruch des Vollzugs führen, unterschieden werden.[51]

---

47 M.E. ist die Sanktionsfolge bei Verlust der Arbeitsstelle differenziert zu betrachten, indem etwa der selbstverschuldete und nicht selbstverschuldete Verlust der Arbeitsstelle unterschiedliche Konsequenzen nach sich zieht, vgl. dazu ausführlich STÖSSEL, 203 sowie 196 f. zur Gleichstellung von Arbeitsloseneinsatzprogrammen; a.A. BSK StGB-KOLLER, Art. 79b N 19 und insbesondere N 29 f.

48 Gl.M. FERREIRA BROQUET, N 117; BSK StGB-KOLLER, Art. 79b N 29; ebenso die Praxis der deutschen und österreichischen Anwendung, vgl. HOCHMAYR, 541 f.; a.A. JOSITSCH/EGE/SCHWARZENEGGER, 329 f., welche dadurch eine unverhältnismässige Einflussnahme einer Drittperson befürchten. Dem kann damit entgegengewirkt werden, dass der Widerruf der Zustimmung nur dann zum Abbruch führt, wenn ein weiteres Eindringen in die Privatsphäre durch das Vollzugspersonal oder aber das Verhalten der überwachten Person als unzumutbar erscheinen und die Rücknahme der Einwilligung somit nicht unbegründet ist, vgl. HOCHMAYR, 542 zur deutschen und österreichischen Praxis.

49 Für eine Übersicht über die kantonalen Regelungen betreffend Verstösse vor Inkrafttreten von Art. 79b StGB vgl. STÖSSEL, 142 ff.

50 Eine solche muss analog den Bestimmungen von Art. 77b Abs. 4 sowie Art. 79a Abs. 6 StGB aus Verhältnismässigkeitsgründen möglich sein, ebenso BSK StGB-Koller, Art. 79b N 30; WERNINGER, 241.

51 Vgl. dazu die Tabelle in STÖSSEL, 205.

ff) Strafcharakter

Im Rahmen des Evaluations-Schlussberichts des interkantonalen Modellversuchs 1999-2002 erfolgte eine Teilnehmerbefragung auch dahingehend, ob der Vollzug mit Electronic Monitoring als Strafe wahrgenommen wurde. Die Ergebnisse zeigten, dass die elektronische Überwachung als Strafe empfunden wurde; insbesondere wurde die Einhaltung des Wochenplans sowie die Übernahme von Eigenverantwortung von den Befragten als Belastung angesehen.[52] Zudem wurde auch erwähnt, dass der ständig zu tragende Sender die Betroffenen rund um die Uhr mit ihrer Situation konfrontierte und regelmässige Blicke auf die Uhr notwendig waren, um den Zeitplan einzuhalten und keinen Alarm auszulösen, was zu einem ständigen physischen und psychischen Druck führte.[53] Die als punitiv empfundene Beschränkung der Bewegungsfreiheit sowie der Gestaltungsfreiheit des Privatlebens wird im Rahmen von Art. 79b StGB durch die Erstellung eines Wochenplans mit festen An- und Abwesenheitszeiten erreicht und bildet damit einen zentralen Aspekt des Vollzugs. Zusätzlich kann der Vollzug auf die individuellen Problembereiche einer Person abgestimmt werden, wodurch neben der Effektivität auch die Punitivität gesteigert wird. Die vielerorts geäusserte Befürchtung, dass der Strafvollzug innerhalb der eigenen vier Wände nicht als Strafe angesehen werden könne, ist diesbezüglich unbegründet und sogar widerlegt. Daran ändert nichts, dass Electronic Monitoring im Vergleich mit dem Normalvollzug als weniger einschneidend empfunden wird, zumal die Beschränkung der Bewegungsfreiheit und der Gestaltungsfreiheit des Privatlebens sowie die Unannehmlichkeiten durch das Tragen des Senders, aber auch die Kontrollbesuche durch das Vollzugspersonal in der Wohnung nicht unerhebliche Eingriffe in die Rechtssphäre des Betroffenen darstellen und damit mit Strafleiden verbunden sind.[54]

b) Electronic Monitoring im Strafprozessrecht

aa) Kontrollinstrument von strafprozessualen Ersatzmassnahmen

Seit Inkrafttreten der eidgenössischen Strafprozessordnung am 1. Januar 2011 wird in Art. 237 Abs. 3 StPO explizit erwähnt, dass das Gericht zur Überwachung von Ersatzmassnahmen den Einsatz technischer Geräte und deren

---

52 e&e, Schlussbericht, 97.

53 e&e, Schlussbericht, 97; vgl. auch Weber, Hausarrest, 213. Für einen Überblick über ausländische Studien zum Thema der Wahrnehmung der Strafelemente von Electronic Monitoring durch die überwachte Person vgl. Stössel, 342 ff.

54 Zum Vergleich der Punitivität mit dem Normalvollzug sowie alternativen Vollzugsformen der Freiheitsstrafe siehe Stössel, 348 ff.

feste Verbindung mit der zu überwachenden Person anordnen kann.[55] Dabei stellt Electronic Monitoring nicht eine eigentliche selbständige Ersatzmassnahme dar, sondern ist vielmehr ein Mittel, um die Ausführung einer Ersatzmassnahme zu kontrollieren, insbesondere von Ein- bzw. Ausgrenzungen nach Art. 237 Abs. 2 lit. c StPO.[56] Für die Anordnung aller Ersatzmassnahmen gelten dieselben Voraussetzungen wie für die Untersuchungs- und Sicherheitshaft, d.h. es ist neben einem dringenden Tatverdacht ein besonderer Haftgrund (Flucht-, Kollusions- oder Wiederholungsgefahr) oder der selbständige Haftgrund der Ausführungsgefahr erforderlich.[57] Zumal der Zweck der Untersuchungshaft primär in der Sicherung der beschuldigten Person und deren Zuführung zur Bestrafung bzw. in der Sicherung von allfälligen Beweisen besteht,[58] unterscheidet sich die Anwendung von Electronic Monitoring zur Überprüfung strafprozessualer Ersatzmassnahmen von derjenigen im Strafvollzug. Während letztere als Arbeits- und Sozialprogramm konzipiert ist, welches einen strukturierten Tagesablauf mit vereinbarten Tätigkeiten und psychosozialer Begleitung beinhaltet, steht bei der Anwendung im Strafprozessrecht der technische, überwachende Aspekt durch Anwendung von GPS-gestütztem Electronic Monitoring im Vordergrund.

Geht man davon aus, dass der Wirkungsmechanismus von Ersatzmassnahmen in der mittelbaren Beseitigung der mit dem besonderen Haftgrund verbundenen Gefahr – etwa durch einen negativen Anreiz in Form einer drohenden Sanktion – besteht, hängt die Wirksamkeit von Ersatzmassnahmen in entscheidender Weise von ihrer Überprüfbarkeit ab.[59] Im Zusammenhang mit dem besonderen Haftgrund der Fluchtgefahr besteht diese Möglichkeit etwa durch die elektronische Überwachung von Eingrenzungen (Art. 237 Abs. 2 lit. c StPO), indem eine eigentliche Flucht zwar nicht verhindert, das Verlassen des im Vornherein bestimmten Rayons aber umgehend ermittelt werden kann, was entsprechend zeitnahe Reaktionen ermöglicht.[60] Im Zusammenhang mit dem Vorliegen von Wiederholungsgefahr würde sich bei ortsspezifischen Delikten etwa eine mittels GPS-Monitoring überwachte Ausgrenzung eignen.[61] Dasselbe gilt für die Minimierung der Kollusionsgefahr, wobei dadurch selbst-

---

55 Vgl. Berlovan, N 34; Schmid/Jositsch, N 1055; BSK StPO-Weber, Art. 237 N 34.

56 Vgl. etwa Urteil des BGer 1B_447/2011 vom 21. September 2011, E. 3.4; Ferreira Broquet, N 554; Manfrin, 276; BSK StPO-Weber, Art. 237 N 35.

57 Vgl. BGE 137 IV 122, E. 2; BSK StPO-Härri, Art. 237 N 2; Schmid/Jositsch, N 1053. Ausführlich zu den besonderen Haftgründen vgl. etwa Donatsch/Schwarzenegger/Wohlers, 190 ff.

58 Vgl. etwa Donatsch/Schwarzenegger/Wohlers, 188.

59 Manfrin, 285 f.

60 BSK StPO-Weber, Art. 237 N 43; vgl. auch Berlovan, N 36.

61 BSK StPO-Weber, Art. 237 N 43; vgl. auch Berlovan, N 42; Manfrin, 281.

verständlich nur die Gefahr unerwünschter physischer Einflussnahme auf Personen oder Beweismittel reduziert werden kann.[62] Nicht zu vernachlässigen ist auch eine präventive Wirkung der elektronischen Überwachung, indem sich die mittels GPS überwachte Person im Bewusstsein befindet, durch die jederzeit mögliche Lokalisation ihres Aufenthaltsortes einem deutlich höheren Entdeckungsrisiko ausgesetzt zu sein.[63]

bb) Bundesgerichtliche Rechtsprechung

Das Bundesgericht steht einer Anwendung von Electronic Monitoring zur Überprüfung strafprozessualer Ersatzmassnahmen offenbar kritisch gegenüber. So beurteilte es die Anwendung von Electronic Monitoring bei Fluchtgefahr – auch in Kombination mit einer Ausweissperre – in mehreren Entscheiden als nicht geeignet, eine Flucht ins Ausland zu verhindern.[64] In einem weiteren Urteil bestätigte das Bundesgericht die Ansicht der Vorinstanz, dass ein Einsatz von Electronic Monitoring in Grenznähe eine Flucht schon aus zeitlichen Gründen nicht zu verhindern vermöge.[65] Dasselbe gilt in Bezug auf die Ausführungsgefahr, indem das Bundesgericht zwar die Möglichkeit einer Überwachung der Einhaltung eines Kontakt- und Rayonverbots nach Art. 237 Abs. 2 lit. g i.V.m. Art. 237 Abs. 2 lit. c StPO mittels Electronic Monitoring erwähnt, jedoch mit dem Hinweis darauf, dass selbst dadurch ein Verstoss nicht zu *verhindern* sei.[66] Nach der Ansicht des Bundesgerichts soll Electronic Monitoring zudem in erster Linie bei Fluchtgefahr, nicht dagegen bei Wiederholungsgefahr zur Anwendung kommen.[67] Ähnliches gilt offenbar in Bezug auf das Vorliegen von Kollusionsgefahr, indem die elektronische Überwachung von der bundesgerichtlichen Rechtsprechung pauschal als „von vornherein ungeeignet, der Kollusionsgefahr entgegenzuwirken" betrachtet wird.[68]

---

62 Vgl. Berlovan, 40; Ferreira Broquet, N 557; ebenso Gfeller/Bigler/Bonin, 715, wonach auch bei Kollusions-, Wiederholungs- und Ausführungsgefahr eine Ein- bzw. Ausgrenzung insbesondere durch die Überprüfbarkeit mittels GPS-gestützter Aufenthaltskontrolle eine taugliche Ersatzmassnahme darstellen kann.

63 Gfeller/Bigler/Bonin, N 712; Vollzugslexikon-Lehner, 146 f.; Manfrin, 281 f.

64 Urteil des BGer 1B_191/2013 vom 12. Juni 2013, E. 3.3; ähnlich auch 1B_4/2013 vom 23. Januar 2013, E. 3.2; 1B_154/2011 vom 27. April 2011, E. 2.3.1 f.; 1B_104/2011 vom 24. März 2011, E. 5.4.

65 Urteil des BGer 1B_172/2013 vom 13. Juni 2013, E. 3; zu Recht krit. Eicker, 351; Manfrin, 278.

66 BGE 140 IV 19, E. 2.6.

67 Urteil des BGer 1B_201/2018 vom 15. Mai 2018, E. 6.

68 Urteil des BGer 1B_50/2019 vom 19. Februar 2019, E. 4.6 mit (erneutem) Hinweis darauf, dass Electronic Monitoring auf die Bannung von Fluchtgefahr zugeschnitten sei, sowie unter Bezugnahme auf das Urteil des BGer 1B_261/2013 vom 11. September 2013, E. 3, wonach Electronic Monitoring (in Form einer Anwesenheitskontrolle mittels *Radiofre-*

Diese Rechtsprechung ist zu kritisieren, wird doch die tatsächliche *Verhinderung* einer Flucht oder von Kollusions-, Wiederholungs- oder Ausführungsgefahr immer nur durch eine Inhaftierung ermöglicht, weshalb bei Beibehaltung dieses Massstabs der Anwendungsbereich von strafprozessualen Ersatzmassnahmen und damit auch deren Überprüfung durch Electronic Monitoring weiterhin minimal ausfallen wird.[69] In einem neueren Urteil des Bundesgerichts wird immerhin davon gesprochen, dass eine Flucht durch Ersatzmassnahmen – Ausweis- und Schriftensperre, elektronische Überwachung von Ein- bzw. Ausgrenzungen und Meldepflicht – im vorliegenden Fall *nicht hinreichend reduziert*, sondern lediglich die Auslösung eines Alarms und eine rasche Entdeckung ermöglicht würde.[70] Dennoch wird von der bundesgerichtlichen Rechtsprechung konsequent ausser Acht gelassen, dass gerade die rasche Entdeckung im Falle eines Verstosses zur Erhöhung der Compliance und damit entscheidend zur Wirksamkeit von Ersatzmassnahmen beiträgt.[71]

Es ist zu wünschen, dass Electronic Monitoring durch die bundesrechtliche Einführung im Bereich des Strafvollzugs am 1. Januar 2018 auch im Bereich der strafprozessualen Anwendungsmöglichkeiten Aufschwung erhält.[72] Die elektronische Überwachung kann dazu beitragen, das Schattendasein von Ersatzmassnahmen in der Praxis zu beenden und damit zur Verwirklichung des Verhältnismässigkeitsprinzips im Zusammenhang mit strafprozessualen Zwangsmassnahmen beizutragen.[73]

---

quenz-Technologie) in Kombination mit einer Ausweis- und Schriftensperre als ungeeignet betrachtet wird, um der Kollusionsgefahr entgegenzuwirken. Dieser Ansicht ist zwar grundsätzlich zuzustimmen, sofern es um die Anwendung einer blossen Anwesenheitskontrolle geht. Es stehen jedoch mit der *GPS-Technologie* längst weitergehende Möglichkeiten zur Verfügung, was im neuen Urteil aus dem Jahr 2019 offenbar verkannt wird.

69 Ebenso Eicker, 351.

70 Urteil des BGer 1B_348/2018 vom 9. August 2018, E. 6.2.5.

71 Gl.M. Gfeller/Bigler/Bonin, 712; Manfrin, 244. Zum Abschreckungseffekt durch elektronische Überwachung ausführlich Stössel, 373 ff.

72 Die Kantone sind verpflichtet, die nötigen Massnahmen zu ergreifen, sodass Electronic Monitoring von einem Gericht angeordnet werden kann, so explizit Urteil des BGer 1B_447/2011 vom 21. September 2011, E. 3.3. Zur Ablehnung wegen fehlender Verfügbarkeit im entsprechenden Kanton vgl. Urteil des BGer 1B_12/2017 vom 3. Februar 2017, E. 2.4; 1B_443/2016 vom 12. Dezember 2016, E. 2.7; 1B_373/2016 vom 23. November 2016, E. 4.3.

73 Stössel, 231 und 305 m.w.N.

c) Electronic Monitoring im Rahmen zivilrechtlicher Gewaltschutzmassnahmen

aa) Anordnung im Rahmen von Art. 28c E-ZGB

Um die Wirksamkeit der zivilrechtlichen Gewaltschutznorm von Art. 28b ZGB zu erhöhen, soll die elektronische Überwachung zur Überprüfung eines gerichtlich angeordneten Annäherungs-, Orts- oder Kontaktverbots angewendet werden können. Ähnlich Art. 237 Abs. 3 StPO handelt es sich bei Art. 28c E-ZGB[74] nicht um eine selbständige Fernhaltemassnahme, sondern um ein Mittel zur Durchsetzung einer Massnahme nach Art. 28b ZGB. Gemäss Art. 28c Abs. 1 E-ZGB kann auf Antrag der klagenden Person[75] die Verwendung einer elektronischen Vorrichtung angeordnet werden, die mit der verletzenden Person fest verbunden ist und mit der ihr Aufenthaltsort *fortlaufend ermittelt und aufgezeichnet* werden kann. Der Wortlaut deutet demnach auf eine passive Überwachung mittels GPS hin, welche keine unmittelbare Intervention durch die Polizei erlaubt.[76] Begründet wird diese Lösung damit, dass im Vergleich zu einer Echtzeitüberwachung weniger personelle und finanzielle Ressourcen benötigt werden; im Gegenzug besteht keine Möglichkeit, die Missachtung von Fernhaltemassnahmen effektiv in Echtzeit zu verhindern.[77] Der Bundesrat ist jedoch der Überzeugung, dass auch mit einer passiven Überwachung der Opferschutz verbessert wird, indem zu erwarten ist, dass sich die gefährdende Person bereits durch das Bewusstsein der Aufzeichnung ihrer Widerhandlungen gegen eine gerichtliche Anordnung an das Annäherungs-, Kontakt- oder Rayonverbot halten wird.[78] Zudem kann der Nachweis einer Missachtung der gerichtlichen Anordnung aufgrund der aufgezeichneten Bewegungsdaten problemlos erbracht werden.[79]

Für die Anordnung der Massnahme ergibt sich aus Art. 28c Abs. 2 E-ZGB eine zeitliche Befristung von sechs Monaten, wobei eine Verlängerung um

---

74 BBl 2018, 7869 f. (Ablauf Referendumsfrist: 7. April 2019).

75 Die Notwendigkeit eines Antrags der klagenden Partei basiert einerseits auf dem im Zivilverfahren geltenden Dispositionsgrundsatz gemäss Art. 58 Abs. 1 ZPO, andererseits gibt die klagende Partei damit aber auch ihre (erforderliche) Zustimmung, ebenfalls ein GPS-gestütztes Gerät auf sich zu tragen, um z.B. ein Annäherungsverbot überprüfbar zu machen.

76 BBl 2017, 7338 und 7345 f. Der Vorentwurf sah offenbar eine aktive Überwachung in Echtzeit vor („[…] mit der ihr Aufenthaltsort dauernd bestimmt werden kann"), so auch explizit Erläuternder Bericht VE, 33.

77 BBl 2017, 7346.

78 BBl 2017, 7346; Zum Abschreckungseffekt durch elektronische Überwachung ausführlich Stössel, 373 ff.

79 BBl 2017, 7346.

jeweils sechs Monate möglich ist. Vorsorglich kann die Massnahme für höchstens sechs Monate angeordnet werden. Art. 28c Abs. 3 E-ZGB verpflichtet zudem die Kantone, die durch eine elektronische Überwachung aufgezeichneten Daten spätestens zwölf Monate nach Abschluss der Massnahme zu löschen.[80] Zudem haben die Kantone eine Zweckbindung zu gewährleisten, damit die aufgezeichneten Bewegungsdaten nur für die Durchsetzung eines Annäherungs-, Orts- oder Kontaktverbots genutzt werden.[81]

bb) Auswirkungen der Anwendung von bilateralem Electronic Monitoring auf das Opfer

Im Zusammenhang mit Art. 28c E-ZGB wird insbesondere befürchtet, dass das Tragen eines GPS-Senders die Frauen „ständig an den Mann, von dem sie sich eigentlich lösen wollten oder müssten", erinnere und die „GPS-Überwachung falsche Sicherheit vorgaukeln" könne.[82]

Die Auswirkungen von bilateralem Electronic Monitoring auf das Opfer, bei welchem die gefährdete ebenso wie die gewaltausübende Person mit einem GPS-Sender ausgestattet wird[83], wurden in einer qualitativen, auf Befragungen von Opfern, Angeklagten und Praktikern in sechs Zuständigkeitsbereichen basierenden, US-amerikanischen Studie von Erez et al. aus dem Jahr 2012 analysiert. Dabei zeigten sich positive Ergebnisse, indem das Bewusstsein, dass die Bewegungen der gefährdenden Person überwacht wurden, als Erleichterung von Belästigungen und Missbrauch empfunden wurde.[84] Zudem stärkte das opferzentrierte bilaterale Electronic Monitoring die Kooperation zwischen den Opfern und den zuständigen Behörden.[85] Dies zeigt, dass neben dem blossen Überwachungsaspekt gerade die persönliche Interaktion des Opfers mit den verantwortlichen Stellen wichtiger Bestandteil einer solchen Anwendung ist. Das Opfer nimmt dadurch eine aktive Position ein, während bei Annäherungs-, Orts- oder Kontaktverboten ohne elektronische Überwachung keine tatsächliche Überprüfbarkeit besteht, wodurch das Opfer in eine passive Rolle des Abwartens gedrängt wird. Diese opferorientierte Massnahme kann folglich

80 BBl 2017, 7347.

81 BBl 2017, 7369; zum Datenschutz im Zusammenhang mit Electronic Monitoring ausführlich Stössel, 313 ff.

82 Merkt, TA vom 27. Januar 2016; ähnlich auch Hunziker, WOZ vom 18. Februar 2016.

83 Vgl. dazu oben, II.2.

84 Erez et al., 144.

85 Erez et al., 142, 152.

neben der Stärkung des Sicherheitsgefühls durch die GPS-Überwachung insbesondere die behördliche Zusammenarbeit mit der gefährdeten Person verbessern.

cc) Ausländische Erfahrungen mit Electronic Monitoring im Bereich häuslicher Gewalt

Obwohl einige Länder bereits Electronic Monitoring im Zusammenhang mit häuslicher Gewalt anordnen, basiert dies i.d.R. auf strafprozessualen Massnahmen, nicht jedoch auf einer zivilrechtlichen Grundlage.[86] Begründet wird dies insbesondere damit, dass eine GPS-gestützte Überwachung massiv in die Persönlichkeitsrechte der zu überwachenden Person eingreift, weshalb solche Massnahmen etwa in Spanien nur bei Straftätern und in Frankreich nur bei der gefährdeten Person zum Einsatz gelangen.[87] Problematisch ist diesbezüglich, dass bei häuslicher Gewalt strafrechtlich oftmals nur Bagatelldelikte vorliegen, das Verhältnismässigkeitsprinzip jedoch die Anordnung von Untersuchungshaft in solchen Fällen verbietet, weshalb die Ergänzung strafprozessualer Massnahmen in Fällen häuslicher Gewalt durch zivil- und polizeirechtliche Gewaltschutzmassnahmen unbedingt notwendig ist.[88] Art. 28b Abs. 1 und 2 ZGB und damit auch Art. 28c E-ZGB beanspruchen somit gerade dann Geltung, wenn strafprozessuale Massnahmen entweder aufgrund des Vorliegens lediglich eines Bagatelldelikts nicht angeordnet werden können oder aber ein über die Untersuchungshaft hinausgehender Schutz notwendig erscheint.

In Anbetracht dessen stellt sich insbesondere die Frage nach der Verhältnismässigkeit. Eine Anwendung von GPS-gestütztem Electronic Monitoring im Rahmen eines zivilrechtlichen Annäherungs-, Orts- oder Kontaktverbots erfordert jedenfalls, dass diese zur Durchsetzung des Verbots geeignet und erforderlich erscheint, insbesondere, weil weniger einschneidende Massnahmen – etwa die Androhung einer Ungehorsamsstrafe gemäss Art. 292 StGB – erfolglos geblieben sind oder von vornherein als ungenügend erscheinen.[89] Eine elektronische Überwachung im Rahmen von Art. 28c E-ZGB scheint somit gemäss Botschaft dann verhältnismässig, wenn bereits ein Verbot nach Art. 28b ZGB angeordnet, diesem jedoch von der gefährdenden Person keine Folge geleistet wurde. Die Aufzeichnung der Bewegungsdaten des Gefährders soll

---

86 BBl 2017, 7393.

87 BBL 2017, 7391; Erläuternder Bericht VE, 20, FN 58; Schweizerisches Institut für Rechtsvergleichung, 95.

88 SCHWARZENEGGER et al., 56 f. m.w.N.

89 BBl 2017, 7346.

dabei ermöglichen, dass das Opfer den Nachweis der Missachtung des gerichtlich angeordneten Verbots problemlos erbringen kann, womit die Durchsetzung der angedrohten Strafe nach Art. 292 StGB erleichtert wird.[90] Dem ist entgegenzuhalten, dass es sich bei Art. 292 StGB lediglich um eine Übertretung handelt, eine GPS-gestützte Überwachung jedoch im Vergleich dazu eine äusserst eingriffsintensive Massnahme darstellt, welche die Bewegungsfreiheit sowie das Recht, über die eigenen personenbezogenen Daten zu bestimmen, einschränkt. Ebenfalls zu kritisieren ist die gemäss Wortlaut von Art. 28c Abs. 2 E-ZGB beliebig verlängerbare Höchstdauer.[91]

Der präventive Einsatz von Electronic Monitoring im Bereich häuslicher Gewalt mag somit auf den ersten Blick verlockend erscheinen. Bei genauerer Betrachtung insbesondere der Verhältnismässigkeit dieser Anwendungsmöglichkeit ist die im Rahmen von Art. 28c E-ZGB mögliche, über das Strafrecht hinausgehende elektronische Überwachung ohne Voraussetzung einer strafrechtlichen Verurteilung jedoch als nicht unproblematisch zu beurteilen.[92]

IV. Spezialpräventive Aspekte von Electronic Monitoring

1. Einfluss von Electronic Monitoring auf die Compliance während des Vollzugs

Gerade bei denjenigen Anwendungsbereichen von Electronic Monitoring, die auf ein dazugehöriges Begleitprogramm verzichten, somit etwa bei der elektronischen Überwachung von strafprozessualen Ersatzmassnahmen oder von zivilrechtlichen Schutzmassnahmen, stellt sich die Frage, ob der Überwachungsaspekt per se einen abschreckenden Effekt aufweist. Dies ist einerseits von Relevanz, da auch mit einer aktiven GPS-Überwachung die Verhinderung einer Straftat nicht zwingend möglich ist, andererseits auch dann, wenn bei einer passiven GPS-Überwachung die Daten nur aufgezeichnet werden, ohne dass eine sofortige Intervention erfolgt, wie dies z.B. im Rahmen der Überwachung zivilrechtlicher Schutzmassnahmen vorgesehen ist.

Diese sog. *instrumentelle Compliance* steht im Zusammenhang mit dem entscheidungstheoretisch angelegten *Rational-Choice*-Ansatz, wonach unser gesamtes Verhalten aus einer rationalen Kosten-Nutzen-Abwägung resultiert.[93] Dabei wird die Entscheidung eines Täters zur Begehung einer Straftat

---

90 BBl 2017, 7346.

91 A.A. Ferreira Broquet, N 829.

92 Ebenso Votum Sommaruga, Amtl. Bull. SR 2011, 357.

93 Vgl. etwa Kunz/Singelnstein, § 12 N 22 ff.

neben der Sanktionshärte insbesondere durch die vermutete Sanktionswahrscheinlichkeit beeinflusst.[94] Gerade hier setzt der Einsatz von Electronic Monitoring an, indem Verstösse sofort feststellbar und so das Entdeckungsrisiko und damit auch die Sanktionswahrscheinlichkeit drastisch gesteigert werden. Die Resultate der Studie von Hucklesby aus dem Jahr 2009, durchgeführt in Nordengland, zeigten, dass die elektronische Überwachung und die dadurch erhöhte Wahrscheinlichkeit einer Strafe im Falle eines Verstosses die Compliance positiv beeinflusste.[95] Gleichzeitig ermöglicht Electronic Monitoring einen objektiven Massstab für die tatsächlich vorhandene Compliance.[96] Eine US-amerikanische Studie von Gies et al. aus dem Jahr 2012 zeigt ähnliche Resultate, indem die Wahrscheinlichkeit von Verstössen gegen Auflagen und Weisungen bei der Kontrollgruppe ohne Electronic Monitoring drei Mal, die Wahrscheinlichkeit eines Rückfalls zwei Mal höher war.[97] Zweifel an der Verlässlichkeit der angewandten Technologie können hingegen einen negativen Einfluss auf die Compliance haben.[98] Es ist deshalb wichtig, dass auf eingehende Alarme eine Reaktion etwa in Form eines Telefonanrufs erfolgt, um zu gewährleisten, dass die überwachte Person die Technologie als verlässlich einstuft. Zudem sind die Folgen bei Pflichtverletzungen durch den Überwachten konsequent durchzusetzen.

2. Bewirken nachhaltiger Verhaltensveränderungen durch Electronic Monitoring

Sobald der Einsatz von Electronic Monitoring in einem konkreten Fall beendet ist, stellt sich die zentrale Frage, ob durch die elektronische Überwachung auch nachhaltige Verhaltensveränderungen bewirkt werden können, somit Verhaltensveränderungen, die auch nach Beendigung der elektronischen Überwachung andauern. Dabei spielt es eine entscheidende Rolle, ob das technische, überwachenden Element von Electronic Monitoring im Vordergrund steht, wie dies etwa bei der Anwendung im Rahmen von zivilrechtlichen Schutzmassnahmen oder im Strafprozessrecht der Fall ist, oder ob Electronic Monitoring – wie bei einem Einsatz im Rahmen von Art. 79b StGB – als Arbeits- und Sozialprogramm konzipiert ist, in welchem die Überwachung an sich nur ein unterstützendes Element darstellt.

---

94 Kunz/Singelnstein, § 12 N 29.

95 Hucklesby, 262.

96 Hucklesby, 267.

97 Gies et al., 5 – 1. Für einen Überblick über weitere Studien zur instrumentellen Compliance und deren Ergebnisse siehe Stössel, 375 ff.

98 Hucklesby, 263.

Denkbar ist, dass das Befolgen eines festen Wochenplans und das Nachgehen einer geregelten Tätigkeit sich unterstützend auf die Selbstkontrolle auswirken und einen Anreiz zum Erlernen nachhaltiger Verhaltenskontrollen setzen kann.[99] Im Sinne der sozialen Lerntheorie[100] kann etwa – wie in der Ausgestaltung von Art. 79b Abs. 1 lit. a und b StGB vorgesehen – positives Verhalten durch progressive Erhöhung der freien Zeit von Beginn bis Ende des Vollzugs mit Electronic Monitoring verstärkt werden.

Fraglich ist, ob ein solcher Effekt auch bei Electronic Monitoring-Konzepten, bei welchen der Kontrollaspekt an sich im Vordergrund steht, ohne in ein Begleitprogramm eingebettet zu sein, eintreten kann. Denn eine Verhaltensänderung auf Basis der sozialen Lerntheorie setzt gerade eine Verstärkung positiven Verhaltens und nicht eine Sanktionierung von Fehlverhalten durch umfassende Kontrolle voraus.[101] Eine Verhaltensänderung erscheint umso weniger realisierbar, je mehr der Kontrollaspekt im Vordergrund steht, ohne dabei mit tagesstrukturierenden und betreuenden Elementen verbunden zu sein. Natürlich steht aber eine nachhaltige Verhaltensänderung bei einem Einsatz von Electronic Monitoring zur Kontrolle von strafprozessualen Ersatzmassnahmen oder zivilrechtlichen Gewaltschutzmassnahmen auch nicht im Vordergrund. Für Electronic Monitoring im Rahmen von Art. 79b StGB ist sie jedoch im Sinne der Rückfallverminderung zentral. Dabei zeigen die Resultate einer Ende 2004 durchgeführten Nachbefragung der Teilnehmer des interkantonalen Modellversuchs von 1999-2002, dass die durchschnittliche Anzahl beibehaltener Verhaltensveränderungen laut Teilnehmern bei 3,92 von sieben[102] erhobenen Bereich lag.[103] Dabei beeinflusste insbesondere die Betreuung während des Vollzugs die Nachhaltigkeit positiv; zudem bestand ein Zusammenhang zwischen positivem Erleben der Verhaltensänderungen und der Beibehaltung derselben.[104] Die Wichtigkeit der Betreuung verdeutlicht, dass bei der Anwendung von Electronic Monitoring im Rahmen von Art. 79b StGB der Kontrollaspekt durch die elektronische Überwachung zwar elementar ist,

---

99 HAVERKAMP/SCHWEDLER/WÖSSNER, NK 2012, 64; SCHWEDLER/WÖSSNER, 12.

100 Zur sozialen Lerntheorie nach BANDURA statt vieler KUNZ/SINGELNSTEIN, § 10 N 6 ff.

101 HAVERKAMP/SCHWEDLER/WÖSSNER, R&P 2012, 16 zur Elektronischen Aufenthaltsüberwachung (EAÜ) in Deutschland, welche im Rahmen der Führungsaufsicht angeordnet werden kann und damit auf sog. *High-Risk Offenders* ausgerichtet ist. Für eine zusammenfassende Darstellung der EAÜ vgl. Stössel, 77 ff.

102 Die sieben Bereiche sind „mehr Eigenverantwortung übernehmen", „Tagesablauf stärker organisieren", „weniger Alkohol trinken", „mehr Zeit zu Hause verbringen", „Problemhilfestellen in Anspruch nehmen", „sich an externe Vertrauenspersonen wenden" und „weniger Zeit im Ausgang/mit Kollegen verbringen".

103 e&e, Nachbefragungen, 12 und 42.

104 e&e, Nachbefragungen, 25 ff.

jedoch mit den anderen Faktoren des Vollzugskonzepts zusammenspielt und vorwiegend stabilisierend auf die Einhaltung der Vollzugsbedingungen einwirkt. Die Ergebnisse der Nachbefragung zum interkantonalen Modellversuch zeigten zudem einen messbaren Zusammenhang zwischen der Nachhaltigkeit von Verhaltensveränderung und Rückfälligkeit, indem sich erstere positiv auf die Rückfallverhinderung auswirkte.[105]

V. Fazit

Der vorliegende Beitrag zeigt auf, dass grundsätzlich sehr weitgehende technische Möglichkeiten bestehen, um sämtliche Bewegungen des Überwachten in Echtzeit nachzuvollziehen. Dabei gilt es zu bedenken, dass selbst mit einer aktiven GPS-Überwachung Straftaten nicht zwingend verhindert, sondern lediglich Verstösse möglichst zeitnah festgestellt werden können, was die Ergreifung vordefinierter Massnahmen ermöglicht. Der Einsatz der elektronischen Überwachung erhöht zudem die Entdeckungswahrscheinlichkeit, was sich positiv auf die Compliance während der Anwendung von Electronic Monitoring auswirkt und damit die überwachte Person darin bestärkt, sich an die entsprechenden Auflagen zu halten. Zudem soll der vorliegende Überblick über den Einsatz der elektronischen Überwachung das Verständnis dafür fördern, dass sich die Ausgestaltungen je nach Anwendungsbereich stark unterscheiden – insbesondere danach, ob das technische Element der Überwachung im Vordergrund steht oder ob der Kontrollaspekt nur einen unterstützenden Faktor in einem Gesamtkonzept darstellt, wie dies im Rahmen von Art. 79b StGB der Fall ist.

Zudem darf nicht ausser Acht gelassen werden, dass nicht alles, was technisch möglich ist, auch in jedem Fall notwendig ist. So kann etwa bei Electronic Monitoring im Strafvollzug im Front Door und Back Door-Bereich, wo fehlende Flucht- und Rückfallgefahr für eine Anwendung vorausgesetzt sind, eine GPS-Überwachung nicht notwendig, für eine Überwachung einer strafprozessualen Ersatzmassnahme oder eines zivilrechtlich angeordneten Annäherungs-, Orts- oder Kontaktverbots aber unbedingt erforderlich sein. Mit einer GPS-Überwachung wird ein ständiges Bewegungsprofil des Überwachten generiert, weshalb zwingend gesetzliche Bestimmungen zur Speicherung und Bearbeitung dieser Daten zu schaffen sind, sofern solche noch nicht bestehen. Technologische Fortschritte sind aber längst Teil unseres Alltags, weshalb

---

[105] e&e, Nachbefragungen, 29 und 43. Für eine detaillierte Auseinandersetzung mit den Auswirkungen von Electronic Monitoring auf die Rückfallwahrscheinlichkeit vgl. STÖSSEL, 389 ff.

ihre Möglichkeiten auch im Bereich der Prävention unbedingt zu nutzen sind, sofern eine sinnvolle, aber auch verhältnismässige Anwendung gewährleistet ist.

Literatur- und Materialienverzeichnis

AEBERSOLD PETER, Is big brother watching you? ZStrR 4/1998, 367 ff.BAECHTOLD ANDREA/WEBER JONAS/HOSTETTLER UELI, Strafvollzug – Straf- und Massnahmenvollzug an Erwachsenen in der Schweiz, 3. Aufl., Bern 2016.

BERLOVAN NATHALIE, L'electronic monitoring en Suisse, Jusletter 19. März 2012.

Botschaft zum Bundesgesetz über die Verbesserung des Schutzes gewaltbetroffener Personen vom 11. Oktober 2017, BBl 2017, 7307 ff.

BRÄGGER BENJAMIN F. (Hrsg.), Das schweizerische Vollzugslexikon – von der vorläufigen Festnahme zur bedingten Entlassung, Basel 2014 (zit. Vollzugslexikon-Bearbeiter).

BROWN TRACY M./MCCABE STEVEN A./WELLFORD CHARLES, Global Positioning System (GPS) Technology for Community Supervision – Lessons Learned, National Institute of Justice, Washington D.C. 2007.

Bundesamt für Statistik, Strafvollzugsstatistiken, Arbeitseinsatz, elektronischer Hausarrest und Betreuung, Stand 09.11.2018, <https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht/justizvollzug/arbeitseinsatz-elektronischer-hausarrest-betreuung.html> (zit. BFS, Electronic Monitoring).

Bundesratsbeschluss über die Verlängerung der Bewilligungen für die Kantone Bern, Solothurn, Basel-Stadt, Basel-Landschaft, Tessin, Waadt und Genf, Freiheitsstrafen in Form des elektronisch überwachten Vollzugs ausserhalb der Vollzugseinrichtung zu vollziehen, 2. September 2015, BBl 2015, 6925 f. (zit. Beschluss BR 2015).

Bundesratsbeschluss über die Bewilligung des Vollzuges von Freiheitsstrafen in Form des elektronisch überwachten Vollzuges ausserhalb der Vollzugseinrichtung für die Kantone Basel-Landschaft, Basel-Stadt, Bern, Genf, Tessin und Waadt vom 28. April 1999, BBl 2000, 3502 (zit. Beschluss BR 2000).

DONATSCH ANDREAS/SCHWARZENEGGER CHRISTIAN/WOHLERS WOLFGANG, Strafprozessrecht, 2. Aufl., Zürich 2014.

e&e Entwicklung und Evaluation GmbH, Interkantonaler Modellversuch Elektronisch überwachter Strafvollzug (EM) für Kurz- und Langstrafen, 1. September 1999 – 31. August 2002, Evaluationsbericht zu den Nachbefragungen, Februar 2007, <https://www.bj.admin.ch/dam/data/bj/sicherheit/smv/monitoring/em-nachbefragungsberichteefeb07.pdf> (zit. e&e, Nachbefragungen).

e&e Entwicklung und Evaluation GmbH, Interkantonaler Modellversuch Elektronisch überwachter Strafvollzug (EM) für Kurz- und Langstrafen, 1. September 1999 – 31. August 2002, Evaluationsbericht zur Rückfalluntersuchung, Dezember 2004, <https://www.bj.admin.ch/dam/data/bj/sicherheit/smv/monitoring/eval-rueckfall-2004-d.pdf> (zit. e&e, Rückfalluntersuchung).

e&e Entwicklung und Evaluation GmbH, Auswertung des interkantonalen Modellversuchs Elektronisch überwachter Strafvollzug (EM) für Kurz- und Langstrafen, 1. September 1999 – 31. August 2002, Evaluations-Schlussbericht, Zürich, 30. Juni 2003, <https://www.bj.admin.ch/dam/data/bj/sicherheit/smv/monitoring/evalres-schlussb-d.pdf> (zit. e&e, Schlussbericht).

Eicker Andreas, Strafprozessrecht/Das Ersatzmassnahmenrecht wird aus den Angeln gehoben – Zur jüngeren Rechtsprechung des Bundesgerichts in Haftsachen, in: Jositsch/Schwarzenegger/Wohlers (Hrsg.), Festschrift für Andreas Donatsch, Zürich 2017, 345 ff.

Erez Edna/Ibarra Peter R./Bales William/Gur Oren M., GPS Monitoring Technologies and Domestic Violence: An Evaluation Study, June 2012, <https://www.ncjrs.gov/pdffiles1/nij/grants/238910.pdf>.

Erläuternder Bericht zum Vorentwurf, Bundesgesetz über die Verbesserung des Schutzes gewaltbetroffener Personen – Erläuternder Bericht zum Vorentwurf, Oktober 2015, <https://www.bj.admin.ch/dam/data/bj/sicherheit/gesetzgebung/gewaltschutz/vn-ber-bg-d.pdf> (zit. Erläuternder Bericht VE).

Ferreira Broquet Ludivine, Le bracelet électronique en Suisse: hier, aujourd'hui et demain, Diss. Univ. Neuchâtel, Basel 2015.

Gfeller Diego R./Bigler Adrian/Bonin Duri, Untersuchungshaft – Ein Leitfaden für die Praxis, Zürich 2017.

Gies Stephen V./Gainey Randy/Cohen Marcia I./Healy Eoin/Duplantier Dan/Yeide Martha/Bekelman Alan/Bobnis Amanda/Hopps Michael, Monitoring High-Risk Sex Offenders with GPS Technology: An Evaluation of the California Supervision Program, Final Report, National Institute of Justice, Bethesda MD 2012.

Haverkamp Rita/Schwedler Andreas/Wössner Gunda, Die elektronische Aufsicht von als gefährlich eingeschätzten Entlassenen, Recht und Psychiatrie 1/2012, 9 ff. (zit. Haverkamp/Schwedler/Wössner, R&P 2012).

Haverkamp Rita/Schwedler Andreas/Wössner Gunda, Führungsaufsicht mit satellitengestützter Überwachung, Neue Kriminalpolitik 2/2012, 62 ff. (zit. Haverkamp/Schwedler/Wössner, NK 2012).

Hochmayr Gudrun, Elektronisch überwachter Hausarrest – Zur Regelung in Deutschland und Österreich, Zeitschrift für Internationale Strafrechtsdogmatik 11/2012, 537 ff.

Hucklesby Anthea, Understanding Offender's Compliance: A Case Study of Electronically Monitored Curfew Orders, Journal of Law and Society 2/2009, 248 ff.

Hunziker David, Sicherheit suggerieren statt Opfer schützen, WOZ vom 18. Februar 2016, <https://www.woz.ch/-687d>.

Jositsch Daniel/Ege Gian/Schwarzenegger Christian, Strafrecht II – Strafen und Massnahmen, 9. Aufl., Zürich 2018.

KKJPD, Electronic Monitoring Mandat der EM-Koordinationsgruppe – 8. Zwischenbericht, Version vom 30.10.2018 (unpubliziertes Dokument; zit. KKJPD, Zwischenbericht EM).

Kunz Karl-Ludwig/Singelnstein Tobias, Kriminologie, 7. Aufl., Bern 2016.

Manfrin Fabio, Ersatzmassnahmenrecht nach Schweizerischer Strafprozessordnung – Ein Beitrag zur Konkretisierung des Verhältnismässigkeitsprinzips im Haftrecht, Diss. Univ. Luzern, Zürich 2014.

Merkt Anita, Die „Fussfessel" allein schützt das Opfer nicht, TA vom 27. Januar 2016, 23.

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar Schweizerische Strafprozessordnung und Jugendstrafprozessordnung, Art. 196-457 StPO und Art. 1-54 JStPO, 2. Aufl., Basel 2014 (zit. BSK StPO-Bearbeiter).

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar Strafrecht I, Art. 1-110 StGB, Jugendstrafgesetz, 4. Aufl., Basel 2018 (zit. BSK StGB-Bearbeiter).

Schlüsselberger Daniel, Electronic Monitoring – eine Übersicht, in: Schwarzenegger/Brunner (Hrsg.), Bedrohungsmanagement – Häusliche Gewalt, Zürich 2018, 75 ff.

Schmid Niklaus/Jositsch Daniel, Handbuch des schweizerischen Strafprozessrechts, 3. Aufl., Zürich/St. Gallen 2017.

Schwarzenegger Christian/Fischbacher Rahel/Loewe-Baur Mirjam/Stössel Jasmine, Häusliche Gewalt, rechtliche Instrumente zum Schutz der Opfer und ihre Wirksamkeit – unter besonderer Berücksichtigung des polizeilichen Gewaltschutzes, in: Schwarzenegger/
Nägeli (Hrsg.), 7. Zürcher Präventionsforum – Häusliche Gewalt, Zürich 2015, 9 ff.

Schwedler Andreas/Wössner Gunda: Elektronische Aufsicht bei vollzugsöffnenden Massnahmen – Implementation, Akzeptanz und psychosoziale Effekte des baden-württembergischen Modellprojekts, Berlin 2015.

Schweizerisches Institut für Rechtsvergleichung, Anzeigeverhalten der Opfer von Straftaten, insbesondere der häuslichen Gewalt und der sexuellen Gewalt gegen Kinder und Jugendliche, Lausanne, 5. April 2012, <https://www.bj.admin.ch/dam/data/bj/sicherheit/gesetzgebung/gewaltschutz/ber-sir-anzeigeverhalten-d.pdf>.

Scottish Government, Development of Electronic Monitoring in Scotland – A Consultation on the Future Direction of the Electronic Monitoring Service, Edinburgh 2013, <https://www.scotland.gov.uk/Resource/0043/00434434.pdf>.

Stössel Jasmine: Electronic Monitoring im Schweizer Erwachsenenstrafrecht – unter besonderer Berücksichtigung der Änderungen des Sanktionenrechts, Diss. Univ. Zürich, Zürich 2018.

Strafvollzugskonkordat Nordwest- und Innerschweiz, Grundlagenpapier vom 22. April 2016 – Möglichkeiten und Grenzen von Electronic Monitoring, <https://www.konkordate.ch/download/pictures/73/47prjg5muj0e7v62p2nzlp837npc2j/moeglichkeiten_und_grenzen_grundlagenpapier_nwi-ch.pdf> (zit. Konkordat Nordwest- und Innerschweiz, Grundlagenpapier EM).

Weber Jonas Peter: Der elektronisch überwachte Hausarrest und seine versuchsweise Einführung in der Schweiz, Diss. Univ. Basel, Basel 2004.

WENNERBERG INKA, High level of support and high level of control – An efficient Swedish model of electronic monitoring?, in: NELLIS/BEYENS/KAMINSKI (Hrsg.), Electronically Monitored Punishment – International and critical perspectives, London/New York 2013, 113 ff.

WERNINGER SOPHIE, Die elektronische Überwachung (Art. 79b StGB), ZStrR 2/2018, 214 ff.

Der digitale Zwilling von Veranstaltungen - App-gestütztes Crowd-Management und Einsatzführung bei Grossveranstaltungen

Ulf Blanke

Inhalt

I. Einleitung

Aktuell leben etwa 50% der Weltbevölkerung in Städten. Bis 2030 steigt dieser Anteil auf zwei Drittel (UN 2014). Die Auswirkungen zeigen sich in der Nutzung des öffentlichen Raums. Wir sehen eine steigende Mobilität mit stärkerem Fluss von Mensch und Material, als auch immer grösser werdende Ansammlungen von Menschen im öffentlichen Raum. Zusätzlich wirken kommerzielle Interessen als Katalysator, Superlative zu erzeugen, insbesondere im Veranstaltungssektor. Es konzentrieren immer mehr und häufiger Menschenmengen im öffentlichen Raum, ein Raum, der oft nicht primär für Veranstaltungen gestaltet wurde. Stadtfeste zum Beispiel ändern binnen Tagen die urbane Funktion und Nutzung von Innenstädten. Strassensperrungen beeinflussen die Mobilität, Veranstaltungspunkte und Attraktionen wirken als neue urbane Funktion und bewirken ein neues kollektives Verhalten der urbanen Bevölkerung. Immer wieder zeigen Beispiele von Menschenkonzentrationen durch

Veranstaltungen erhebliche Sicherheitsprobleme. Oft resultieren diese durch Fehlplanung, aber auch durch Fehleinschätzungen von Besucherverhalten. Multipliziert man also das Verhalten von einzelnen mit 100'000 bis Millionen Besuchern, erzeugt dies eine starke Herausforderung die Sicherheit zu erhalten und fordert neue Mittel zur Bewältigung.

In diesem Beitrag fokussieren wir uns speziell die Gewährleistung von Sicherheit an Grossveranstaltungen, wie zum Beispiel Stadtfesten, Sportveranstaltungen oder Festivals. Die Komplexität der Sicherung einer Grossveranstaltung entspricht einer taktischen Operation mit einer hohen Zahl an Beteiligten und hohem Grad an Rollen. Der Erfolg hängt dabei von einem gut kommunizierenden Team und Organisationen ab als auch von angemessener Information- und Kommunikations-Technologien (IKT).

Überraschenderweise, und obwohl IKT-Systeme für Command and Control Anwendungen bereits seit Jahrzehnten in Militär und in der öffentlichen Sicherheit eingesetzt werden, ist die Nutzung für Grossveranstaltungen im Zusammenspiel mit privaten Dienstleistern für die Veranstaltungssicherheit kaum existent. Die Gründe dafür sind mehrdimensional. Zum einen erfüllen existierende IKT-Systeme die benötigte Agilität, Funktion, und Einfachheit der Nutzbarkeit nicht. Zum anderen ist die unflexible Preisstruktur nicht marktgerecht für den Sicherheitsmarkt. Niedrige Margen und die Unterschiedlichkeit der Einsätze benötigen einen neuartigen Ansatz sowohl in Funktionalität als auch in der Kommerzialisierung.

Somit findet sich ein Status Quo in der Veranstaltungssicherheit vor, welcher aus einfachen Kommunikationsmitteln wie Funkgerät oder Telefon bestehen. Als Konsequenz ist die Führung als „Knotenpunkt" der Kommunikation besonders beansprucht. Stress-verursachend kann dies zu Fehlern, und letztendlich zu unvorhergesehenen Katastrophen führen, wie an der Love-Parade in Duisburg.

Um die Herausforderungen zu bewältigen fokussieren wir uns auf die Aspekte *Situationsbewusstsein*, *Aufmerksamkeitslenkung* und *Analysierbarkeit*. Im Codesign[1] haben wir im engen Austausch mit Sanitätsdienste, Sicherheitsdienstleistern, und Behörden antavi Ops[2] entwickelt. Durch diese partizipative Software Entwicklung konnten neue Technologien genau auf die Anforderungen abgebildet werden.

Zusätzlich bringen wir den Begriff der *empfundenen Sicherheit* des Besuchers als wichtigen Bestandteil in der Prävention. Nicht jeder Besucher empfindet

1 Sanders.

2 <https://www.antavi.ch>.

beispielsweise Körperkontakt in dichten Situationen als unsicher. Andere hingegen können darauf panisch reagieren, wenn dies nicht erwartet wurde. Dementsprechend ist es notwendig Erwartungen der Besucher rechtzeitig zu managen.

Als Ergebnis entsteht dabei ein „digitaler Zwilling". Durch transparente Informationsflüsse wird in Echtzeit die physische Welt virtuell wiedergespiegelt und in einem Feedback-Loop ein Informationskreislauf mit allen Akteuren einer Veranstaltung erzeugt. Nur dann lässt sich die Komplexität der Veranstaltungssicherheit beherrschen.

1. Grossveranstaltung als „Komplexes System"

Auf Grossveranstaltungen spielen viele *Akteure* eine Rolle für das Gesamtverhalten. Zu diesen Akteuren gehört jeder einzelne Besucher, jedes Team-Mitglied der Sicherheits- und Sanitätsdienste, als auch das Gesamt-Management der Veranstaltung. Jeder Akteur zeigt dabei eine Entscheidung und Verhalten. Diese sind bereits in Planung absehbar. Zum Beispiel, bestimmt der Festplan den Besuch einer bestimmten Band, oder der Raum und Weggestaltung die Wegfindungsentscheidung. Das Verhalten kann dabei beeinflusst werden durch Folge oder Leitverhalten gegenüber anderen Akteuren. Bei diesem Zusammenspiel zwischen Akteuren,[3] den sogenannten *lokalen Interaktionen* entsteht ein *emergentes* Verhalten der Gesamtmasse, bzw. des *Systems*. Man bezeichnet solche Verhaltens-Systeme als *komplexe* Systeme,[4] da sie im Verhalten sehr schwierig bis unmöglich vorherzusehen geschweige denn zu steuern sind. Mit dieser Erkenntnis liegt die Frage nahe, wie man das Verhalten einer Menschenmenge besser oder überhaupt steuern kann.

Zum einen ist eine *globale* Sicht wichtig. Zum anderen, eine klar orchestrierte Leitung verteilter Akteure. Nur in einem klar abgestimmten Zusammenspiel aller Akteure kann ein komplexes System „quasi-global" gesteuert werden, und damit zum einfachen System gewandelt werden.

2. Technologischer Status quo

Betrachtet man eingesetzte Technologien in der Veranstaltungssicherheit, sieht man sehr oft eine einfache Ausstattung. Teams im Feld werden mit einem Walkie Talkie ausgestattet und müssen bei Vorfällen per Funk verbal die Ereignisse beschreiben. Das erfordert eine zentrale Gegenstelle, welche manuell die

---

3 Corrado; Treuille.

4 Corrado; Luo.

Gesamtsituation alle Akteure zusammenfasst, Entscheidungen trifft und diese als Interventionsanweisung zurückspielt. Als Knotenpunkt der Kommunikation liegt die Intuition nahe, dass die Leitstelle einen starken Engpass definiert. Ereignisse zu erfassen und zu aggregieren erzeugt eine hohe kognitive Belastung und Zeitdruck. Zudem behindern Kommunikationsschwierigkeiten von gefunkten Nachrichten aufgrund fehlender Funk-Ausbildung die schnelle und präzise Darstellung einer Situation oder eines Ort des Ereignis. Dementsprechend erschwert der Status quo die Bemächtigung des komplexen Systems. Denn meist bleiben Kompetenzen isoliert bei den Akteuren, statt zentral effizient orchestriert zu werden.

Im Gegensatz zur privaten Sicherheit ist die Digitalisierung von Einsätzen in der öffentlichen Sicherheit oder im Militär bereits seit Jahrzehnten in der Entwicklung und kommerziell verfügbar. *Abbildung 1* zeigt verschiedene Leitzentralen ausgestattet mit komplexen Kommunikations und Echtzeit-Geo-Informationssystemen. Sogenannte Systeme für *Command*, *control*, *communications*, *computers and intelligence* (C4I) sind weit verbreitet mit zahlreichen technologischen Anbietern.

Abbildung 1 Leitzentralen in der öffentlichen Sicherheit und im Militär.

Hexagon, Bosch, Raytheon, Siemens, Motorola, Sunguard, Huawei sind nur einige Anbieter. Für Grossveranstaltungen im Zusammenspiel mit privaten Sicherheitsanbietern sind diese Systeme allerdings ungeeignet. Fehlende Agilität, eine komplexe Bedienung und markt-ungerechte Kosten machen solche Systeme nicht nutzbar. Zudem verfügen diese Systeme nicht über offene Schnittstellen, so dass der Bürger oder Besucher nicht partizipieren kann, wie wir später in diesem Beitrag beschreiben. Wir betrachten den Kreislauf von Sicherheitspersonal und Besuchern als wichtigen Bestandteil im Crowd-Management und in der Veranstaltungssicherheit und entwickeln dementsprechend offene Technologien. Bevor in Kapitel III ein neuartiges System für die Veranstaltungssicherheit vorgestellt wird, nehmen wir im nächsten Kapitel Bezug zu neuen Technologien. Diese bilden die Basis für neuartige Systeme für die Veranstaltungssicherheit.

II. Neue Technologien

Mit der Entwicklung in der Mikroelektronik und Software-Entwicklung traten eine Reihe neuer Anwendungsmöglichkeiten auf den Markt. Gleichzeitig generieren tragbare Endgeräte und Umgebungs-Sensoren Daten, welche durch Anwendung von maschinellem Lernen Erkenntnisse liefern. Durch Open Data Initiativen werden Daten von Dritten zugreifbar und können eigene Daten anreichern. In diesem Kapitel wird zunächst die Möglichkeiten des Smartphones vorgestellt.

Im zweiten Teil, erläutern wir die wichtige Rolle von Open Data. Im letzten Teil gehen wir auf neue Techniken der Datenverarbeitung ein, um aus einer Fülle von Daten Erkenntnisse zu ziehen und unterschiedliche Datenquellen für Sicherheit und Prävention, insbesondere in Hinblick auf Grossveranstaltungen, nutzbar zu machen.

1. Smartphone und Sensoren

In nur einer Dekade hat sich das Smartphone weltweit verbreitet. Nahezu 80%[5] der westlichen Bevölkerung besitzen ein Smartphone und tragen es täglich mit sich. Noch vor wenigen Jahren unvorstellbar, enthalten gängige Smartphones eine Reihe von Sensorik. In Serie ausgestattet besitzen diese GPS-Lokalisierung, ein Bluetooth-Modul zur Gerätekommunikation und Inertialsensorik zur Bewegungserfassung. Mit der GPS-Lokalisierung lässt sich zum Beispiel aus schon wenigen lokalisierten Appbenutzer Dichten und Bewegungsdynamiken ganzer Besuchermengen abschätzen.[6] Mit Bluetooth-Scans können Gruppierungen erfasst werden, als auch die Menschendichte, die sich in der Umgebung eines Gerätes befindet.[7] Beschleunigungssensoren können dabei die Bewegung erfassen. Zum Beispiel lässt sich abschätzen ob eine Person steht, geht, rennt[8] oder ob sie hingefallen ist[9] und unbeweglich auf dem Boden liegt. Mit Tonaufnahmen mittels Smartphone-Mikrofon lassen sich weiterhin aus Umgebungsgeräuschen automatisch die Stimmung der Umgebung charakterisieren.[10] Auch können Umgebungsgeräusche Rückschlüsse auf Besucherdichten liefern.[11] Wie man aus Rohdaten, wie zum Beispiel einem

5 New Zoo Global Mobile Market Report 2018.

6 Blanke.

7 Weppner.

8 Shoaib.

9 Abbate.

10 Chon.

11 Elhamshary; Kannan.

Beschleunigungssignal (siehe *Abbildung 7*) oder einer Audio-Aufnahme automatisch ein Verhalten ableiten oder eine Besucherdichte bestimmen kann, wird in Abschnitt II.4. erläutert.

Neben der Sensorik bieten Smartphones heutzutage die Rechenleistung eines Desktop-Rechners. Zudem sind sie permanent mit dem Internet verbunden. Damit wird das Smartphone fähig das Verhalten des Benutzers wahrzunehmen, zu analysieren und in nahezu Echtzeit weltweit zu kommunizieren. Aggregiert über mehrere Benutzer können Aussagen über kollektives Verhalten getroffen werden. Damit wird ein Netzwerk von Smartphones das „Nervensystem" des komplexen Systems.

Um das Auslesen und Verarbeiten von Smartphone-Daten zu ermöglichen, benötigt es eine App, welche mit Programmlogik, Daten erfasst und versendet. Gleichzeitig ermöglichen Apps die Interaktionen zwischen Akteuren (z.B. durch Push-Benachrichtigungen oder Messaging). Durch Vertriebsplatformen wie Apple Appstore oder Google Playstore, wird die Distribution solcher Apps einfach und ermöglicht eine weltweite Verbreitung. Neben Smartphones spielen auf Internet der Dinge (Internet of Things) eine tragende Rolle als angewendete Technologie in diesem Beitrag. Im nächsten Abschnitt gehen wir auf verschiedene Beispiele ein, wie „Dinge" wahrnehmen und miteinander kommunizieren, und Teil des digitalen Zwillings werden.

2. Internet of Things

Die Vision von Internet of Things ist es physische und digitale Gegenstände miteinander zu verbinden und durch IKT interagieren zu lassen. Wir zeigen an Beispielen wie das Internet of Things Bezug in der Sicherheit nimmt.

Wie eingangs erwähnt besteht eine Grossveranstaltung aus Akteuren, welche im Zusammenspiel ein komplexes Verhalten erzeugen. Mit Smartphones kann dieses Verhalten durch Smartphone-Sensorik wahrgenommen werden, als auch gesteuert werden. Nebst tragbarer Sensorik liefern auch Sensoren aus der Umgebung Daten. Ein Beispiel zeigt *Abbildung 2*. Über CCTV Kameras werden Objekte klassifiziert und gezählt. Diese werden in einem Geografisches Informations-System (GIS) visualisiert und Statistiken erfasst. Damit werden Trends unmittelbar sichtbar, ohne dass, das Personal jemals das Kamera-Bild – das Rohmaterial – sehen und analysieren muss. Durch aufmerksamkeitssteuernde Warnungen, kann schnell auf die Situation reagiert werden.

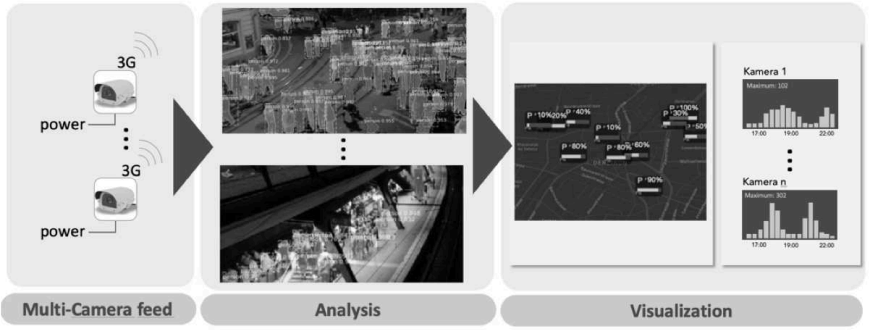


Abbildung 2 Automatische Bestimmung von Besucherdichten aus einem Kamera-Netzwerk mittels maschinellen Lernens.

3. Open Data und Datenfusion

Open Data bezeichnet die Initiative Daten zur Weiterverarbeitung und zur Verwendung von jedermann frei zugänglich zu machen. Das Ziel von frei nutzbarem Daten ist es, mehr Transparenz und Zusammenarbeit, als auch Verbesserungen von Dienstleistungen zu schaffen für öffentliches oder privates Interesse. Datensätze können dabei aus geografischen Datenbanken kommen, aus Statistik-Instituten, oder beispielsweise aus Verkehrsinformationen mit Ursprung in privatwirtschaftlichen Unternehmen, als auch in öffentlichen Stellen. Wir zeigen wie die Zusammenführung verschiedener Datenquellen genutzt werden kann, um Erkenntnisse für Grossveranstaltungen und die verbundene urbane Mobilität zu gewinnen. Daraus kann kontextbewusste Informationen für Besucher als auch Sicherheitspersonal gewonnen werden, um bedarfsgerecht und in Echtzeit handeln zu können.

Geodatenbanken. Jedes Smartphone kann GPS-Koordinaten des Standorts erfassen. Bestehend aus einer numerischen Breiten- und Längengradangabe, z.B. 47° 22’ 36.7968” N8° 32’ 30.0984” E, hat diese noch keine semantische Bedeutung für den Menschen. Um diese Zahl zu interpretieren, benötigt es Geo-Daten in Form von Kartenmaterial. Open Streetmap[12] beinhaltet eine offene Datenbank bestehend aus dem kompletten Strassennetz und Strecken des öffentlichen Verkehrs. Eine weitere Datenbank „Foursquare[13] bietet Informationen über nächst-gelegene Plätze, wie Sehenswürdigkeiten, Restaurants, oder Gebäuden, gegeben einer GPS Koordinate.

12 <http://www.openstreetmap.org>; HAKLAY.

13 <https://enterprise.foursquare.com/products/places>.

Aber was genau ermöglicht dies? *Abbildung 3* zeigt links eine Sammlung von GPS Punkten, welche von Smartphone Benutzern gewonnen wurde und zu zeitgestempelten Sequenzen verbunden wurden. Neben Genauigkeitsfehlern einzelner Punkte (hier bis zu 200m) enthalten GPS-Sequenzen Unterbrechungen, so dass eine genaue Analyse der Mobilität mit nur dieser Datenquelle unmöglich scheint. Nach einem sogenannten *matching* auf das Strassennetz mittels Openstreet-Map werden jedoch Wegstrecken sichtbar (*Abbildung 3 Mitte*). Zusammen mit Geschwindigkeitsparametern erlaubt dies die Unterscheidung der Transport-Modalität: z.B. die Nutzung eines Fahrzeugs, Fahrrad oder des öffentlichen Verkehrs (Mitte). Mit Aggregation über viele Benutzer, kann dann die Belastung des gesamten Netzes sichtbar gemacht werden (*Abbildung 3 Links*): Die Liniendicke visualisiert die Stärke der Strassenabschnitts-Belastung.

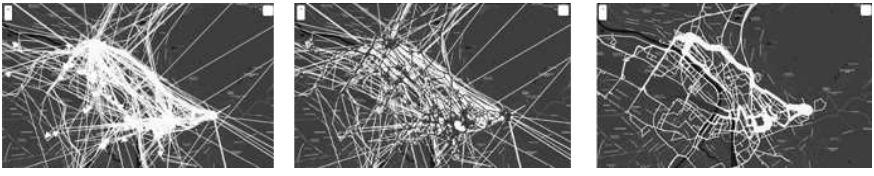


Abbildung 3 Erfasste GPS-Trajektorien (links) werden durch OpenStreetmap auf das Strassen-Netz abgebildet (mitte), für die Erfassung der meistgenutzten Wegstrecken (rechts).

Abbildung 4 Parkleitsystem Zürich. Interne Ansicht (rechts) und In-App Ansicht für Besucher (Züri Fäscht App 2019)

Mit einer Mobilitäts-Analyse wird in Echtzeit das Bewegungsverhalten sichtbar. Dies ist für Veranstaltungen ohne klare Start- und Endzeit bedeutsam und ermöglicht die An- und Abreise Optimierung angepasst an Bedürfnisse von Besuchern.

Verkehrsinformationen. Immer mehr Städte machen Ihre Parkleitsysteme offen. Damit kann die Anzahl freier Parkplätze erfasst werden. Durch Open-Data Schnittstellen können diese, z.B., für die Verkehrsführung als auch für den Benutzer zugänglich gemacht werden (siehe *Abbildung* 4). Dies findet, z.B., beim Züri Fäscht 2019 Anwendung in der Züri Fäscht App, mit mehr als 2M Besuchern an einem Wochenende. Mit Kenntniss voller Park-Garagen, lassen sich unnötige Anfahrten vermeiden und damit auch ein Stauaufkommen präventiv reduzieren.

Besucherdaten. Grossveranstaltungen oder Festivals beinhalten oft ein komplexes Programm. Besucher haben dabei im Vorfeld häufig Präferenzen, wann und was sie erleben wollen. Wenn man dieses Wissen bereits erfasst, kann die Attraktivität von Orten und Programmpunkten prognostiziert werden.

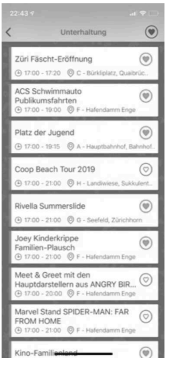


Abbildung 5 Beispiel Züri Fäscht App mit favorisierbaren Programmpunkten

Damit kann Sicherheitspersonal präventiv und bedarfsgerecht eingesetzt werden. *Abbildung* 5 zeigt am Beispiel der Züri Fäscht App, wie Benutzer Programmpunkte favorisieren können. Favoriten werden zentral für alle Benutzer gespeichert und pro Programmpunkt gezählt.

Festplätze	Programmpunkte
• 373 likes for HIVE FLIEGT AUS • 325 likes for FRIEDA'S BÜXE • 261 likes for Electronic Musik Festival „Graue Gasse“ • 172 likes for KAUFLEUTEN meets PÖSTLI am Züri Fäscht • 156 likes for Züri Fäscht am Zähringerplatz mit Terrazzza, Erika The Piñata & BaBaLu	• 714 likes for Musikalisches Feuerwerk „Silver eyes – Hymne an den Mond“ um Freitag 22:30-23:00 • 477 likes for Musikalisches Feuerwerk „Schlager Festival“ um Samstag 22:30-22:50 • 402 likes for ewz-Drohnenshow um Freitag 00:15 – 00:25 • 390 likes for Musikalisches Feuerwerk „Only Rock“ um Samstag 01:00-01:20 • 373 likes for HIVE FLIEGT AUS um Freitag ab 22:00

Tabelle 1 Beispiel: Züri Fäscht App Daten von Usern, welche bestimmte Festplätze und Programmpunkte für den Besuch favorisiert haben.

Dadurch lassen sich wie in Tabelle 1 Statistiken von favorisierten Programmpunkten (Top 5) über alle Benutzer erzeugen und durch Sortierung eine Rangliste bestimmt werden. Durch die zusätzliche Verortung der Programmpunkte kann entsprechend eine geografische Häufigkeitsverteilung des erwarteten Publikums visualisiert werden. *Abbildung* 6 zeigt dies für Programmpunkte des Züri Fäscht 2019. Damit kann der Veranstalter Platz-, Personal- und Mobilitätsbedürfnisse bereits im Vorhinein abschätzen.

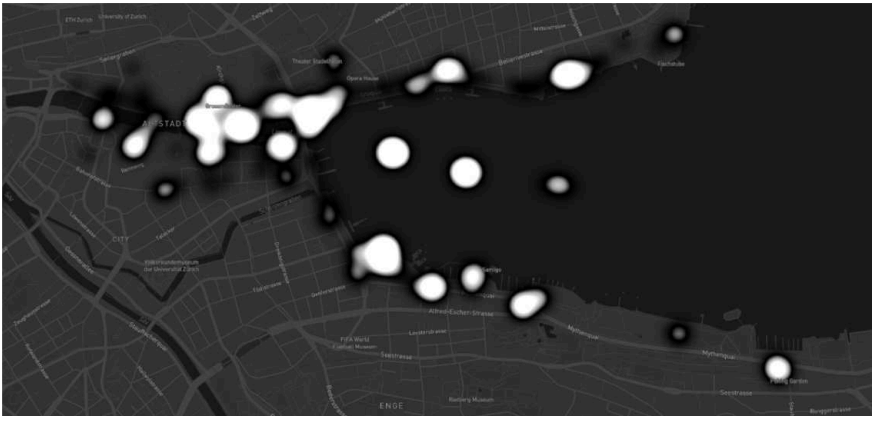


Abbildung 6 Beispiel: Favorisierte Programmpunkte als Heatmap dargestellt. Je mehr Benutzer einen Programmpunkt favorisieren, desto heller die Heatmap.

Nimmt man all diese heterogenen Informationen zusammen ergeben sich neuartige Analysemöglichkeiten für die Mobilität und Ansammlungen von Menschenmengen. Durch die Integration solcher Informationen in den Kontext der Benutzer, werden Informationen für die Situation relevant und wertvoll.

4. Maschinelles Lernen, Data Mining und Visualisierungs-Techniken

Mit der Entwicklung von immer leistungsfähiger Hardware und die stetig wachsenden Datenmassen, sind auch neue Methoden in der Software-Entwicklung entstanden, um diese zu bewältigen und nutzbar zu machen.

In Teil II.1 wurde eine Auswahl von Sensoren vorgestellt, die in gängigen Produkten wie dem Smartphone oder der Smartwatch zu finden sind. Zum Beispiel reagiert ein Beschleunigungssensor auf Bewegung und erzeugt dabei Zeitserien von Beschleunigungswerten. Menschliches Bewegungsverhalten kann dabei sehr genau charakterisiert werden. *Abbildung* 7 zeigt eine solche Beschleunigungs-Zeitserie während verschiedener Aktivitäten durchgeführt werden. Mit dem Auge sind bereits Trends im Signal zu erkennen, welche mit dem Verhalten korrelieren. Um diese automatisch auswerten zu können werden Mittel des Maschinellen Lernens verwendet.

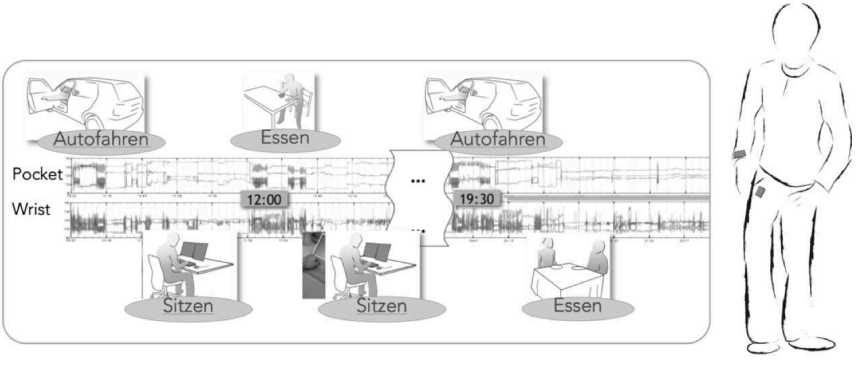


Abbildung 7 Beschleunigungsdaten von zwei Sensoren am Handgelenk (Smartwatch) und in der Tasche (Smartphone)

Dabei werden zunächst Merkmale im Signal berechnet. Die kann zum Beispiel die Varianz des Signals sein oder der Mittelwert über einen definierten Zeitabschnitt. Um ein System für die automatische Erkennung von Bewegungsklassen zu trainieren, werden diese Abschnitte mit der Verhaltensklasse annotiert. Sprich zu jedem Zeitabschnitt, wird festgehalten, welche Aktivität die Person

zu dem Zeitpunkt durchgeführt hat. Diese Annotationen werden dann mit den Rohdaten, respektive den errechneten Merkmalen, einem System zum Training gegeben. Man kann sich das vorstellen, als lerne man eine neue Sprache wobei der Datensatz aus Rohdaten und Annotation einem Vokabelheft entspricht. Hat das System genug Beispiele gelernt, kann es bei Präsentation ungesehener Rohdaten eine Schätzung vornehmen, welches Verhalten diese neuen Daten entsprechen könnten.

Mit diesem Verfahren können Rohdaten automatisch maschinell klassifiziert werden. Dabei ist die Methode uneingeschränkt anwendbar auf Beschleunigungsdaten, Audio-Daten, GPS-Daten oder anderen Daten. Zum Beispiel lassen sich dadurch aus GPS-Zeitserien abschätzen, welches Verkehrsmittel die Person genutzt hat. Parameter im GPS-Signal, durch Sensorfusion mit Beschleunigungssignalen, als auch die Anreicherung mit OpenDaten wirken wie eine Signatur der Mobilität (zu Fuss, rennend, Fahrrad, PKW, Bus oder Bahn).

Auch lässt sich automatisch die Dichte durch maschinelle Auswertung (Computer Vision) von Kamerabildern ermitteln.[14]

Durch die Leistungsfähigkeit der Smartphones können Daten direkt auf dem Smartphone verarbeitet werden, so dass lediglich die Klassifikation übertragen wird. Bei diesem sogenannten *Edge Computing* findet die Verarbeitung am Rande des Netzwerks statt (auf dem Smartphone) im Gegensatz zum *Cloud Computing*. Erst später werden vorverarbeitete Daten in der Cloud über mehrere Benutzer aggregiert, um Aussagen über kollektives Verhalten zu treffen.

Der letzte Schritt ist die Visualisierung grosser Datenmengen. Diese spielt eine tragende Rolle in der Interpretierbarkeit und Aufmerksamkeitssteuerung. In *Abbildung* 8 sind einige Beispiele zu Geo-Daten abgebildet. Zum Beispiel wird aus vielen GPS Punkten eine Heatmap erzeugt mit einem Kerndichteschätzer (links oben). Dadurch lassen sich Hotspots farblich hervorheben. Flowlines (unten) zeigen Menschenflüsse in verschiedenen Liniendicken. Die Dicke spiegelt die Menge der Personen wider, welche die Routen nutzen. Sparklines[15] zeigen Trendlinien und heben letzte Änderungen hervor, siehe Parkleitsystem in *Abbildung* 4. Das sind nur einige Beispiele von möglichen Visualisierungstechniken, neben klassischen Zeitreihen zur Visualisierung historischer Daten.

14 Albakour; Kong.

15 Tufte.

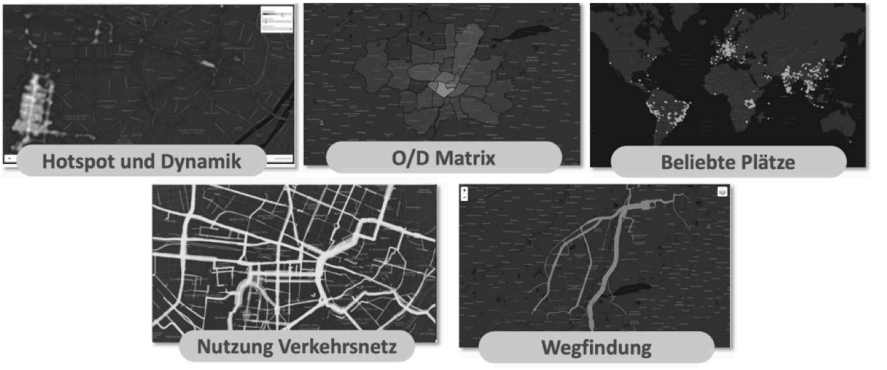


Abbildung 8 Analyse- und Visualisierung zur Crowd- und Mobilitäts-Analyse während Grossveranstaltungen

In diesem Kapitel wurde vorgestellt wie das Zusammenspiel von Sensorik, das Anreichern mit Daten Dritter (OpenData) und Software Methoden zur maschinellen Verarbeitung ein System „wahrnehmen" und die Aufmerksamkeit des Menschen gezielt auf relevante Informationen ausrichten kann. Damit lassen sich Entscheidungen schneller treffen, bei gleichzeitig reduzierter kognitiver Belastung. Die Realität bekommt ein digitales Abbild – den digitalen Zwilling. Dieses kann jederzeit wieder abgespielt und analysiert werden, um potentielle Ereignisse und Fehler zu verstehen und in Zukunft zu vermeiden.

III. Antavi Ops Leitzentrale für Veranstaltungen

Mit den genannten Technologien und der steigenden Vernetzung entwickeln sich auch die Anwendungsfelder. Mit der Möglichkeit durch Sensoren wahrzunehmen, maschinell die Aufmerksamkeit zu steuern und durch gezielte Informationsflüsse Akteure zu informieren, entsteht ein Informations- und Daten-Kreislauf (siehe *Abbildung* 10). Dabei finden Handlungs-Entscheidungen bei allen Akteuren statt: bei dem steuernden Sicherheitspersonal, als auch bei dem Besucher selbst. Durch transparente Kommunikation und Erwartungsmanagement der Besucher können diese selbst Entscheidungen durchführen, ob und wie sie Veranstaltungen erleben wollen. Das führt zum Begriff der *empfundenen Sicherheit.*

Abbildung 9 Beispiel für In-App Kommunikation an Benutzer in Bezug auf Besucherdichten

Durch Fehlerwartungen kann eine Situation als sicherheitsbedrohlich empfunden, welche objektiv betrachtet nicht unbedingt eine Sicherheitsbedrohung enthält. Zum Beispiel kann vermehrter Körperkontakt in einem Gedränge als unangenehme Erfahrung bereits Einfluss auf das Sicherheitsempfinden haben und als Konsequenz sicherheitsbedrohliches Verhalten verursachen. Statt auszuharren kann eine panische Reaktion gefährliches Drängeln und Drücken auslösen. *Abbildung* 9 zeigt am Beispiel des Züri Fäscht, wie Besucherdichten transparent vermittelt werden. Neben einem einfachen Füllgrad-Indikator wird zusätzlich eine Beschreibung kommuniziert, welche Erwartungen beschreibt. Damit können Besucher sich einstellen und selbst entscheiden bei welcher Besucherdichte ihr Sicherheitsempfinden positiv bleibt. Als Konsequenz lassen sich überraschende Angst-Situationen vermeiden, und daraus resultierende Folgeereignisse vermeiden.

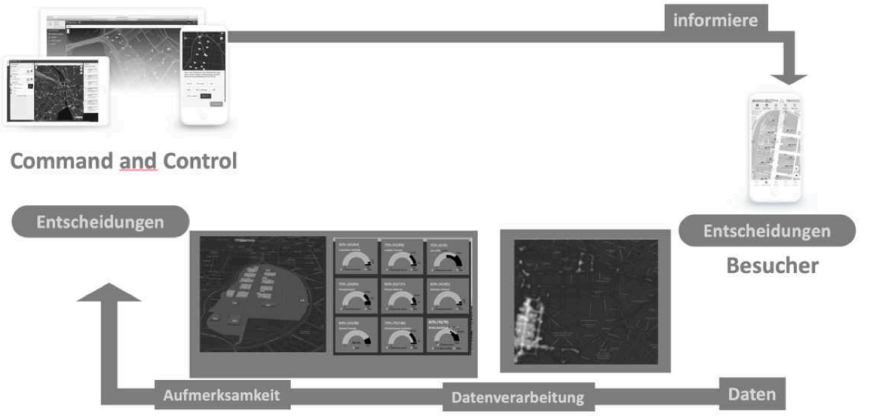


Abbildung 10 Daten- und Informations-Kreislauf und Entscheidungseinfluss auf das Handeln.

1. Kommunikation zwischen Team-Mitgliedern

Ein klarer und schneller Kommunikationsweg ist grundlegende Basis für ein erfolgreiches Sicherheits-Management auf Grossveranstaltungen. Wie eingangs erwähnt reduziert sich die Kommunikation auf den meisten Veranstaltungen auf das Funkgerät. Das birgt Nachteile, insbesondere für ungeschultes Personal, welches sich in einer Stresssituation mit einer klaren verbalen Kommunikation konfrontiert sieht. Mit antavi Ops, wird der Kommunikationsweg erweitert, so dass das Sicherheits-Management zu jederzeit den Ort des Personals einsehen kann. Gleichzeitig ermöglicht die georeferenzierte Kommunikation eine einfache und schnelle Kommunikation, so dass der Funk-Kanal schneller frei wird und die kognitive Belastung der Ereignis-Aufnahme, der Analyse der Situation und der Reaktion deutlich reduziert wird.

2. Analysierbarkeit der Sicherheit

Protokollierung geschieht oft nur händisch auf Papier, und verteilt auf die verschiedenen Akteure und Organisationen. Eine Zusammenfassung dieser Materialien ist dabei aufwendig und eine klare Analyse durch unstrukturierte Speicherung nahezu unmöglich. Durch die zentrale Speicherung lässt sich das aufwendige Zusammenstellen aus heterogenen Materialien vermeiden. Durch strukturierte Speicherung lassen sich einfach Ereignis und Verhaltens-Analysen herstellen. Die Auswertung (siehe *Abbildung 13*) kann dabei wichtige Hinweise liefern auf den Sicherheitsbedarf. Zum Beispiel: Sind meine Sicher-

heitsposten an optimaler Stelle positioniert? Ist die Belastung einzelner Sanitätsposten gleichverteilt? Wieviel Zeit wird benötigt, um ein Ereignis abzuarbeiten? Gibt es noch Pendenzen, die im Ereignisfall abzuarbeiten sind?

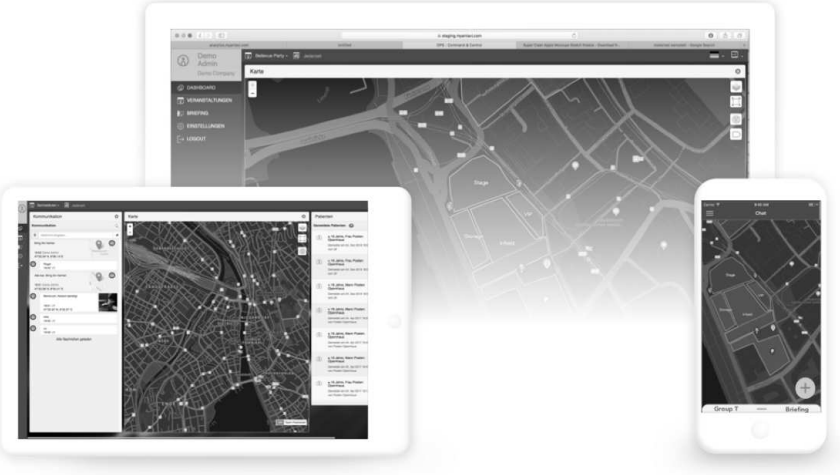


Abbildung 11 Command and Control System „antavi Ops“ im Desktop-Browser und als App für Smartphone und Tablet.

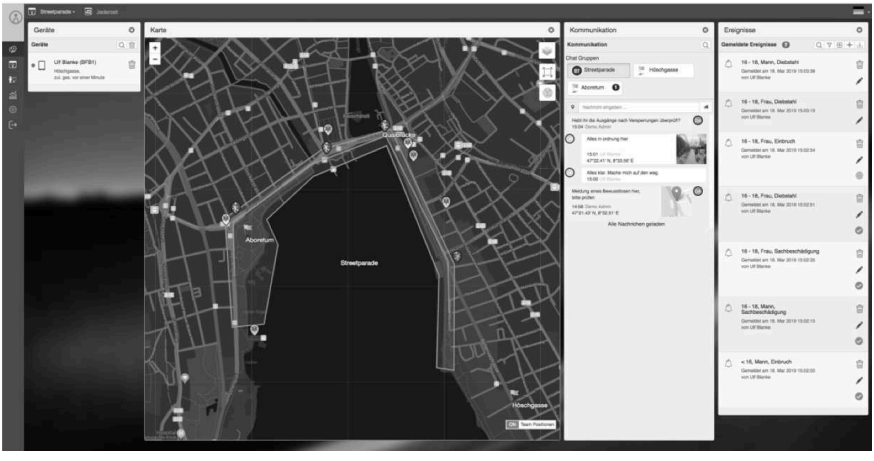


Abbildung 12 Taktische Kommunikation in Echtzeit. Jede Information, z.B. Chat-Nachricht, Bild, oder Ereignisse werden automatisch georeferenziert und auf einer Karte schnell lokalisierbar.

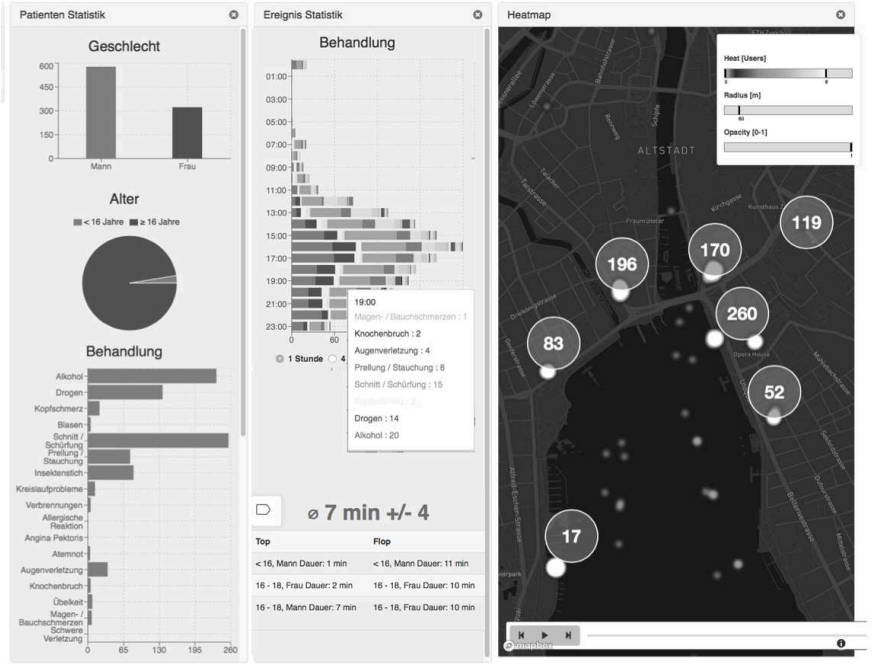


Abbildung 13 Die Analyse-Ansicht ermöglicht unter anderem die Auswertung von Ereignis-Arten, die Verarbeitungsgeschwindigkeit und geografische Häufigkeit.

Neben operativen Funktionalitäten, die auf den Prozess der Veranstaltungssicherheit abgestimmt sind, spielt bei grossen Teams, die Administration eine wesentliche Rolle bei der Durchführung. Vereinfacht gesagt läuft die Sicherheit in folgendem Ablauf statt: (1) Einsatzvorbereitung, (2) Briefing zur Einsatzbesprechung, (3) Einsatzdurchführung, und (4) Einsatz-Debriefing. Um auch vor dem Einsatz die Vorbereitung möglichst effizient durchzuführen, wurde der Teamaufbau und Briefing digitalisiert. *Abbildung 14* zeigt dabei wie in Vorbereitung Teams und Rollen, z.B. Sanitäter oder Bewachung, definiert werden können. Jede Rolle ist mit einem QR Code verbunden, so dass sich Personal ohne aufwendige Registrierung anmelden und gebrieft werden können. QR-Codes enthalten eine Gültigkeitsdauer, so dass nach Ablauf, z.B. nach Veranstaltungsende, das Personal automatisch ausgeloggt werden. Da Teams temporär eingesetzt werden und oft in neuer Zusammensetzung, wurde auf ein Benutzermanagement verzichtet. Dies beschleunigt den Teamaufbau und das Zugriffsmanagement deutlich.

Abbildung 14 QR-Code Registrierung für effiziente Administration und Entlastung des Sicherheits-Managements

3. Antavi Ops Im Einsatz

Antavi Ops wird von verschiedenen Nutzergruppen auf Veranstaltungen genutzt: Sanitätsdienste, Sicherheitsdienste, als auch öffentliche Einrichtungen wie Polizei und Schutz und Rettung. Antavi Ops kam bereits bei mehr als 30 Veranstaltungen in der Schweiz zum Einsatz und wird zunehmend in der gesamten Schweiz eingesetzt (siehe *Abbildung* 15).

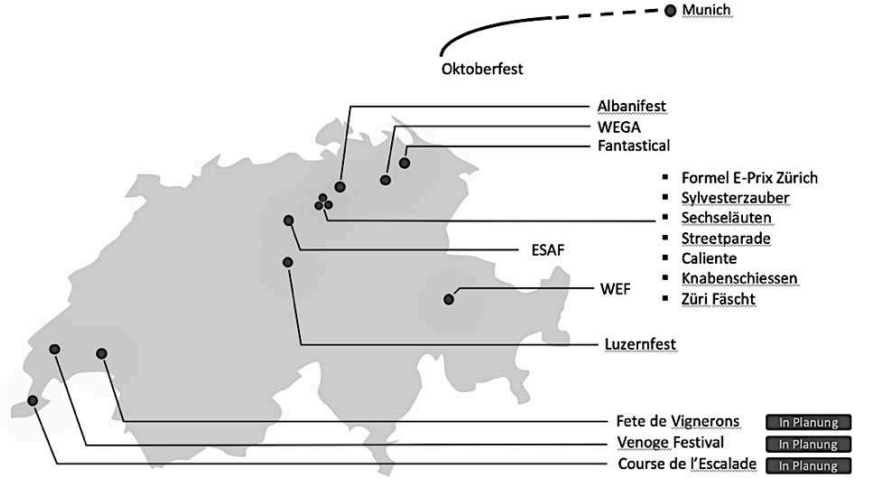


Abbildung 15 Einsatzorte und Events von antavi Ops

Abbildung 16 und *Abbildung* 17 zeigen Impressionen innerhalb des Lagezentrums, welche antavi Ops nutzen. Man sieht dabei den sehr einfachen Aufbau für den schnellen temporären Einsatz: Die Software für das Lagezentrum läuft als Web-Applikation im Browser und kann per Beamer im Lagezentrum dargestellt werden. Die Software ist unter stetiger Weiterentwicklung mit dem Ziel einer standardisierten Funktionalität für den Einsatz auf Veranstaltungen und im Krisenmanagement[16] zu definieren.

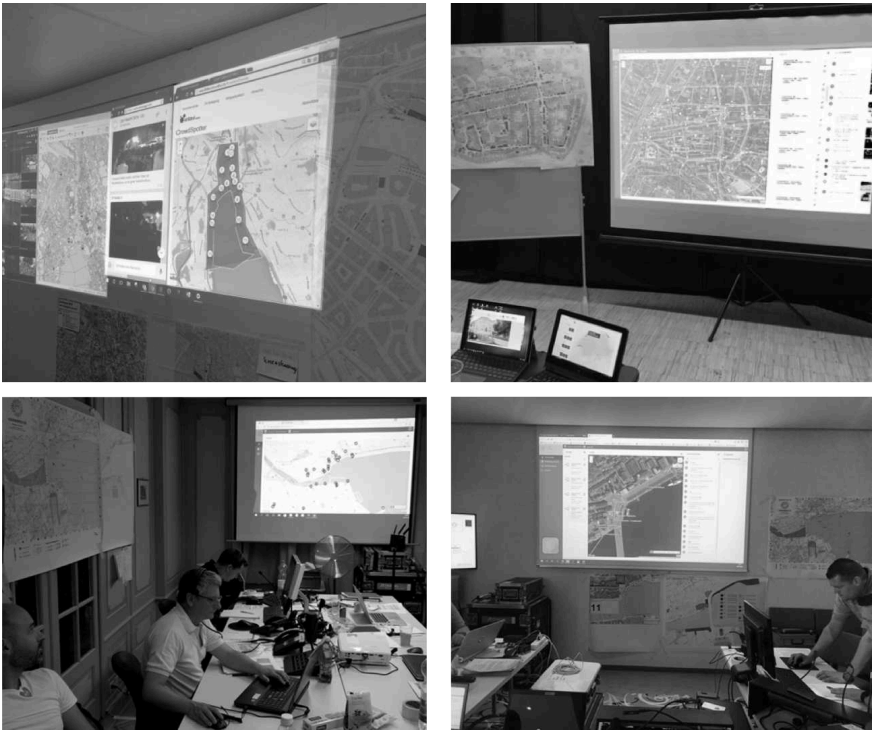


Abbildung 16 Impressionen des Einsatzes in Sicherheits-Leitzentrale des Organisation-Komitees: (Unten) Luzerner Fest 2017, 2018. (Oben rechts) Albani-Fest 2018 und Züri Fäscht 2016 (Oben links)

16 <https://www.antavi.ch>.

Abbildung 17 Impression Züri Fäscht 2016: Während Schichtwechsel mit Blick auf aktuelle Besucherdichte für bedarfsgerechten Einsatz mobiler Einheiten (Bildschirm Hintergrund)

IV. Zusammenfassung

In diesem Beitrag wurde die Rolle von neuen Technologien im Zusammenspiel für die Veranstaltungssicherheit dargestellt. Dabei entsteht ein *digitaler Zwilling* der Veranstaltung, welcher alle physischen Elemente und Aktivitäten virtuell wiederspiegelt. Damit wird das Situationsbewusstsein verbessert und die Reaktionsgeschwindigkeit erhöht. Auch steht der Besucher mit Entscheidungskomponente als auch als Datenlieferant in einer zentralen Rolle. Durch Erwartungsmanagement wird dem Besucher klar, wie er das Fest für sich erleben kann und sein Verhalten an sein eigenes Sicherheitsempfinden anpassen kann. Mit der neuartigen Kombination aus einem Digitalen Zwilling für besseres Situationsbewusstsein, einem Informationskreislauf, der alle Akteure verbindet und Entscheidungen optimal unterstützt und durch effiziente Kommunikationslösungen, wird ein optimaler Prozess für die Veranstaltungssicherheit gestaltet, der jetzt und n Zukunft für mehr Sicherheit und Komfort auf Grossveranstaltungen sorgt.

Literaturverzeichnis

Abbate S./Avvenuti M./Bonatesta F./Cola G./Corsini, P./Vecchio A., A smartphone-based fall detection system, Pervasive and Mobile Computing 8(6) 2012, 883-899.

Albakour M./Macdonald C./Ounis I., Using sensor metadata streams to identify topics of local events in the city, in: Proceedings of the 38th International ACM SIGIR Conference on Research and Development in Information Retrieval 2015 (August), 711-714.

Blanke U./Tröster G./Franke T./Lukowicz P., Capturing crowd dynamics at large scale events using participatory gps-localization, in: 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2014 (April).

Corrado A.J., Dynamics of complex systems, CRC Press 2019.

Chon Y./Lane N.D./Li F./Cha H./Zhao F., Automatically characterizing places with opportunistic crowdsensing using smartphones, in: Proceedings of the ACM Conference on Ubiquitous Computing 2012 (September), 481-490.

Elhamshary M./Youssef M./Uchiyama A./Hiromori A./Yamaguchi H./Higashino T., CrowdMeter: Gauging congestion level in railway stations using smartphones, Pervasive and Mobile Computing 2019.

Haklay M./Weber P., Openstreetmap: User-generated street maps, IEEE Pervasive Computing 7(4) 2008, 12-18.

Kannan P.G./Venkatagiri S.P./Chan M.C./Ananda A.L./Peh L.S., Low cost crowd counting using audio tones, in: Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems 2012 (November), 155-168, ACM.

Kong D./Gray D./Tao H., A viewpoint invariant approach for crowd counting, in: 18th International Conference on Pattern Recognition (ICPR'06), Vol. 3, 2006 (August), 1187-1190, IEEE.

Luo L./Zhou S./Cai W./Low M.Y.H./Tian F./Wang Y./Xiao X./Chen D., Agent-based human behavior modeling for crowd simulation, Computer Animation and Virtual Worlds 19(3-4) 2008, 271-281.

Sanders E.B.N./Stappers P.J., Co-creation and the new landscapes of design. Co-design 4(1) 2008, 5-18.

Shoaib M./Scholten H./Havinga P.J., Towards physical activity recognition using smartphone sensors, in: 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, 2013 (December), 80-87, IEEE.

Treuille A./Cooper S./Popović Z., Continuum crowds, ACM Transactions on Graphics (TOG) 25(3) 2006, 1160-1168.

Tufte E.R., The visual display of quantitative information (Vol. 2). Cheshire: CT: Graphics press 2001.

UN D., World urbanization prospects: The 2014 revision, United Nations Department of Economics and Social Affairs, Population Division: New York 2015.

Weppner J./Lukowicz P./Blanke U./Tröster G., Participatory bluetooth scans serving as urban crowd probes, IEEE Sensors Journal 2014, 4196-4206.

Fahrerassistenzsysteme - Verkehrsunfallprävention und neue Risiken

Bettina Zahnd

I. Einleitung

In modernen Personenwagen werden zahlreiche Fahrerassistenzsysteme verbaut. Häufig als Komfortsystem verkauft helfen einige Systeme Unfälle zu vermeiden. Der Nutzen von Fahrerassistenzsystemen für die Verkehrsunfallprävention wird anhand von drei Systemen für Personenwagen und einem System für Motorräder aufgezeigt.

Personenwagen werden zunehmend automatisiert. Beim Übergang von Fahrzeugen, die von Menschen gelenkt werden zu selbstfahrenden Fahrzeugen, werden neue Unfallursachen erwartet. Neue Risiken können zu Unfällen führen. Die Risiken frühzeitig zu erkennen und Massnahmen zu deren Minimierung zu ergreifen, wird wichtig sein, um das generelle Unfallvermeidungspotential der zunehmend automatisierten Fahrzeuge ausschöpfen zu können.

II. Grundlagen und Methoden

Die Frage danach, wie viele Unfälle mit einem gewissen Fahrerassistenzsystem verhindert werden können, ist nicht einfach zu beantworten. Unfälle, die verhindert werden konnten, werden nicht registriert. Der Nachweis erfolgt deshalb indirekt. Entweder indem man vergleicht, wie viele Unfälle mit oder ohne System verursacht werden oder indem man Unfälle im Detail analysiert, den Unfallhergang bestimmt und anschliessend simuliert, wie der Hergang sich verändert hätte, wenn ein bestimmtes Fahrerassistenzsystem eingegriffen hätte. Für die Analyse stehen verschiedene Datenquellen zur Verfügung. Verwendet wurden einerseits Daten des Bundesamtes für Strassen und andererseits Versicherungsdaten.

1. Fahrerassistenzsysteme

Der Fokus der Untersuchungen liegt auf vier unterschiedlichen Fahrerassistenzsystemen, welchen aufgrund von theoretischen Überlegungen zur Häufigkeit von Unfällen und zur Wirkungsweise der Assistenzsysteme ein hoher Nutzen zugeschrieben wird.

a) Anti-Blockier-Bremssystem (ABS) für Motorräder

Die ersten ABS für Motorräder wurden bereits 1988 eingeführt, damals als teure Zusatzoption. Seit 1. Januar 2016 müssen neue Modelle und seit 1. Januar 2017 alle neu zugelassenen Motorräder ab 250cm3 mit einem ABS ausgerüstet sein. ABS verhindert das blockieren der Räder, indem der Bremsdruck verringert wird, falls ein Rad blockiert und wieder erhöht wird, wenn das Rad wieder frei dreht. ABS beim Motorrad führt in erster Linie dazu, dass das Motorrad während der Bremsung stabil bleibt und so die Sturzgefahr minimiert wird. Zudem wird der Bremsweg verkürzt, weil die Räder dank der Elektronik maximal gebremst werden ohne dass sie blockieren.

b) Elektronisches Stabilitätsprogramm (ESP) für Personenwagen

ESP wurde Ende 1990er Jahre entwickelt. Serienmässig eingeführt wurde es bei Mercedes, nachdem die damals neue A-Klasse bei einem Bremsausweichtest in Schweden – dem Elchtest – auf die Seite kippte. ESP unterstützt den Fahrer, indem der Fahrerwunsch via Lenkwinkelsensor überprüft wird und mit der tatsächlichen Fahrtrichtung verglichen wird. Stellt das System eine Abweichung fest, wird gezielt an einem Rad die Bremskraft erhöht, so dass ein Drehmoment in die entgegengesetzte Richtung entsteht. Das Fahrzeug wird so wieder in die gewünschte Fahrtrichtung gedreht. ESP verhindert, dass das Fahrzeug bei abrupten Lenkmanövern oder bei etwas zu schnellen Kurvenfahrten ins Schleudern gerät.

c) Notbremsassistent für Personenwagen

Notbremsassistenzsysteme wurden in den 00er Jahren entwickelt und sind seither in unterschiedlichen Ausbaustufen verfügbar. Ein Notbremsassistent ist ein vorausschauendes Fahrerassistenzsystem, welches den Fahrer vor einer drohenden Kollision warnt und das Fahrzeug – falls der Fahrer nicht reagiert – selbstständig abbremst. Das Notbremsassistenzsystem von Volvo, welches in dieser Arbeit näher untersucht wird, kann bei guten Strassenverhältnissen Kollisionen verhindern, also das Auto vollständig zum Stehen bringen, bei denen die Relativgeschwindigkeit des vorderen Fahrzeugs und des Volvos bis maximal 30km/h beträgt. Bei Relativgeschwindigkeiten bis 60km/h kann die Unfallschwere vermindert werden.

d) Parksensoren für Personenwagen

Parksensoren sind aktive Einparkhilfen, die auf Ultraschallsensoren basieren. Eingeführt wurden sie bereits 1982 bei Toyota. Die Parksensoren errechnen die Distanz zum erkannten Hindernis und warnen den Fahrer, wenn eine gewisse Distanz unterschritten wird. Parksensoren sind somit die ursprünglichste Art der Einparkhilfen, welche heute mehr Funktionalitäten anbieten, wie z.B. Rückfahrkameras oder Systeme, die selbst abbremsen, sobald ein Hindernis erkannt wurde. In dieser Arbeit wurde auf Parksensoren fokussiert, bei denen der Fahrer nur gewarnt wird.

2. Datengrundlagen

Welchen Nutzen Fahrerassistenzsysteme haben, wurde anhand von zwei Datensätzen überprüft, den Daten des ASTRAs und den eigenen Versiche-

rungsdaten. Die Datenquellen unterscheiden sich insbesondere durch die Art der Erhebung, die schwere der Unfälle, die erfasst wird, und die Datentiefe, die vorhanden ist. Beide Datenquellen haben Vor- und Nachteile.

a) ASTRA Daten

Die Daten, die das ASTRA interessierten Nutzern zur Verfügung stellt, werden von der Polizei mittels Unfallaufnahmeprotokoll erfasst und ans Bundesamt für Strassen weitergeleitet. Seit dem 1.1.2018 wird das Unfallaufnahmeprotokoll 2018 verwendet, davor das etwas ausführlichere Unfallaufnahmeprotokoll 2011.[1]

Das Bundesamt für Strassen stellt Standardstatistiken zur Verfügung, welche einen Überblick über das Unfallgeschehen geben.

Das Bundesamt für Statistik stellt die Daten zur weiteren Analyse zur Verfügung. Ein kostenloser Zugang ermöglicht eigene Auswertungen der Daten in den Verschiedenen Datenwürfeln, z.B. zu Unfallbeteiligten oder zu Unfällen. Mit dem kostenpflichtigen Zugang ist eine Verknüpfung der Unfallbeteiligten und der Unfälle möglich.[2]

Die ASTRA Daten umfassen alle Unfälle, bei denen die Polizei den Unfall aufgenommen hat. Folglich sind fast alle Unfälle, bei denen mindestens eine Person verletzt oder getötet wurde in der Statistik enthalten. Die Dunkelziffer von Unfällen mit Verletzten oder Getöteten, die nicht von der Polizei aufgenommen wurden, wird als sehr klein geschätzt. Anders sieht es bei Unfällen aus, bei denen nur Sachschaden entstanden ist. Solche Unfälle werden teilweise von der Polizei aufgenommen, teilweise auch nicht. Ob die Polizei den Unfall aufnimmt oder nicht hängt von diversen Faktoren ab. Die Unfallbeteiligten müssen bei Unfällen ohne Personenschaden nicht zwingend die Polizei rufen. Es scheint, als ob auch kantonale Unterschiede bestehen bei der Aufnahme von Unfällen mit reinen Sachschäden.

Die Datenbank eignet sich somit sehr gut, um Unfälle mit Personenschaden auszuwerten, sie sagt aber wenig aus über Unfälle mit reinem Sachschaden.

b) Versicherungsdaten

Die Verkehrsunfalldaten der Versicherer umfassen alle Unfälle, bei denen ein Personenwagen haftpflichtig war. Das heisst insbesondere, wenn ein Perso-

---

1 ASTRA.

2 bfs.

nenwagen Sachschaden verursacht hat, Unfälle, bei denen der Hauptschuldige der Versicherungsnehmer ist, aber auch Unfälle, bei denen eine Betriebshaft festgestellt wird. Letztere Fälle beinhalten zum Beispiel Unfälle zwischen Personenwagen und Fussgängern, auch wenn die Hauptschuld nicht beim Personenwagenlenker liegt.

AXA als grösster Motorfahrzeugversicherer der Schweiz mit knapp einem Viertel Marktanteil erhält somit rund einen Viertel aller Unfälle, bei denen ein Personenwagen involviert war. Auch in dieser Datenbank gibt es eine Dunkelziffer von Unfällen, die nicht gemeldet werden, weil der Schaden unter dem Selbstbehalt (für Privatpersonen in der Regel je nach Vertrag zwischen CHF 0.– und 1000.–) liegt. Die Dunkelziffer ist aber klar kleiner als bei den Daten des ASTRAs.

In einer Studie der Hochschule für Technik und Gestaltung Konstanz (HTWG) und der AXA aus dem Jahr 2009 wurden 574 Schadenfälle im Detail untersucht und kategorisiert. Als Basis dienten alle Unterlagen zum Schadenfall, was meist die Fotos der Beschädigungen der Fahrzeuge, der Unfallort, die Aussagen beider Parteien und falls vorhanden den Polizeirapport beinhaltete. Ein Student hat im Rahmen seiner Bachelorarbeit die 574 Schadenfälle kategorisiert und festgestellt, dass nach den Unfällen beim Parkieren und Manövrieren (rund 37% der Unfälle) die Auffahrkollisionen als zweithäufigster Unfalltyp 20% der Unfälle ausmachen.

3. Retrospektive und prospektive Studien

Um das Potential von Fahrerassistenzsystemen zu beurteilen, werden im Wesentlichen zwei Methoden unterschieden. Bei retrospektiven Studien wird rückblickend die Unfallfrequenz, also die Häufigkeit der Unfälle bezogen auf die Exposition, betrachtet. Es wird verglichen, mit welcher Häufigkeit Fahrzeuge mit einem spezifischen Fahrerassistenzsystem und Fahrzeuge ohne dieses Fahrerassistenzsystem Unfälle verursachen. Die Schwierigkeit bei dieser Methode liegt darin, dass bekannt sein muss, welches Fahrzeug über welche Systeme verfügt hat. Am einfachsten gelingt diese Unterscheidung bei Fahrzeugen, die generell oder ab einem gewissen Baujahr serienmässig mit dem Fahrerassistenzsystem ausgerüstet sind. Beachten muss man zusätzlich, dass ähnliche Fahrzeuge miteinander verglichen werden, bei denen auch die Fahrerpopulation so ähnlich wie möglich ist.

Prospektive Studien eignen sich dann, wenn sehr viele Details zu Unfällen ohne das Fahrerassistenzsystem zur Verfügung stehen, zum Beispiel, wenn Unfälle ohne Fahrerassistenzsystem von einem Unfallsachverständigen analysiert wurden und ein Gutachten vorliegt. In diesen Fällen kann simuliert wer-

den, wie das Fahrzeug mit einem spezifischen Fahrerassistenzsystem reagiert hätte. Die Simulation zeigt dann auf, ob der Unfall mit diesem System hätte verhindert werden können, ob die Unfallfolgen gemindert worden wären oder ob das System keinen Einfluss gehabt hätte.

III. Resultate zum Nutzen von Fahrerassistenzsystemen

Vier Fahrerassistenzsysteme wurden in unterschiedlichen studentischen Arbeiten in Zusammenarbeit zwischen AXA und der HTWG in Konstanz untersucht. Eine prospektive Studie zum ABS für Motorräder und drei retrospektive Studien zum Notbremsassistenten, zu ESP und zu Parksensoren.

1. Prospektive Studie zum ABS für Motorräder

Die Grundlage für die Studie zum ABS für Motorräder aus dem Jahr 2009 bildeten 65 Motorradunfälle, bei denen Motorräder ohne ABS verunfallt sind. Die Unfälle geschahen in einem Zeitraum von 2007-2008. Jeder einzelne dieser Unfälle lag als Gutachten von einem Sachverständigen der AXA vor. Die Gutachten beschrieben den genauen Hergang der Motorradunfälle. Von den 65 Motorradfahrern konnten lediglich 45% vor der Kollision bremsen. Da das ABS für Motorräder nur wirken kann, wenn überhaupt eine Bremsung vorliegt, wurden nur diejenigen Fälle weiter untersucht, bei denen der Motorradfahrer bremsen konnte. Von denjenigen, die bremsen konnten, sind 59% der Motorradfahrer nicht gestürzt. ABS hätte auch in diesen Fällen eine grosse Wirkung gehabt, diese lässt sich jedoch schwer rekonstruieren. Bei Bremsungen mit dem Motorrad kann die Bremsverzögerung auch von einem Unfallanalytiker nur annähernd bestimmt werden. Wie viel grösser sie mit ABS gewesen wäre, lässt sich aufgrund mangelnder Fakten nicht simulieren. Für die verbleibenden 41%, die gestürzt sind, wurde die Simulation durchgeführt. Es wurde berechnet, wie lange der Bremsweg mit ABS gewesen wäre und ob das Motorrad vor der Kollisionsstelle hätte anhalten können. Gemäss Simulation hätten 75% derjenigen Motorradfahrer, die vor dem Unfall bremsen konnten und dabei gestürzt sind, den Unfall mit ABS verhindern können. Bei den restlichen 25% der Unfälle hätten mit ABS die Unfallfolgen gemindert werden können.

In den untersuchten 65 Motorradunfällen hätten folglich fast 14% der Unfälle komplett vermieden werden können. In den restlichen 27% der Unfälle, in denen der Fahrer Bremsen konnte, hätte ABS die Unfallfolgen mindern können.

2. Retrospektive Studie zum ESP für Personenwagen

In einer studentischen Arbeit 2016 wurden gleich drei Fahrerassistenzsysteme retrospektiv untersucht. Für die Untersuchung der Wirksamkeit des Elektronischen Stabilitätsprogramms ESP wurden die Unfälle des Dacia Sanderos Modell 2008 ohne ESP, welche in den Jahren 2008- 2014 verursacht wurden, mit den Unfällen des Dacia Sanderos Modell 2012 mit ESP, welche in den Jahren 2013-2015 verursacht wurden, verglichen. Aus all den Unfällen, die in diesen Zeitperioden mit diesen Fahrzeugen verursacht wurden, wurden alle Selbst- und Schleuderunfällen bei Fahrgeschwindigkeiten, also ohne Manövrierunfälle, in die Untersuchung eingeschlossen. Total wurden über 2.5 Mio versicherte Tage einbezogen. Die Anzahl relevanter Unfälle pro versicherten Tag der beiden Dacia Sandero Modelle wurden verglichen. Das Resultat: mit dem Dacia Sandero mit ESP wurden 47% weniger Schleuderunfälle verursacht als mit dem Dacia Sandero ohne ESP.

3. Retrospektive Studien zum Notbremsassistenten für Personenwagen

Bis heute hat AXA zwei unterschiedliche retrospektive Studien zu Notbremsassistenten für Personenwagen erstellt. Bereits im Jahr 2011 wurde eine Studie zum ersten serienmässig eingebauten Notbremsassistenten des Volvo XC60 erstellt. Im Jahr 2016 wurde ein bereits weiterentwickeltes Notbremsassistenzsystem, welches in der B-Klasse serienmässig eingeführt worden war, untersucht.

a) Studie 2011 – Volvo XC60 mit City Safety

Der Volvo XC60 war das erste Modell, welches serienmässig über einen Notbremsassistenten verfügte. Für die Studie wurden die bei der AXA gemeldeten Unfällen des Volvo XC60 und sechs weiteren, kleinen Small Utility Vehicles (SUVs) untersucht. Die Vergleichsfahrzeuge waren der Audi Q5, der BMW X3, der Mazda CX7, der Mercedes GLK, der Lexus RX und der VW Tiguan. Total wurden 866 Unfälle kategorisiert und die Häufigkeit von Auffahrkollisionen der sieben SUVs verglichen. Im Vergleich zum Durchschnitt der anderen sechs kleinen SUVs haben die bei AXA versicherten Volvo XC60 mit Notbremsassistent 30% weniger Unfälle verursacht.

Limitierend bei dieser Studie ist, dass davon ausgegangen werden muss, dass die Fahrer der verschiedenen kleinen SUVs ein unterschiedliches Fahrerprofil aufweisen.

b) Studie 2016 – Mercedes B-Klasse mit Collision Prevention Assist (CPA)

Für die Untersuchung des CPA von Mercedes wurden die Unfälle der Mercedes B-Klasse Modell 2005 ohne CPA im Zeitraum von 2008-2011 und der Mercedes B-Klasse Modell 2011 mit CPA im Zeitraum von 2012-2015 verglichen. Aus allen Unfällen, die im entsprechenden Zeitraum gemeldet wurden, wurden die Auffahrkollisionen als relevante Unfälle für die Studie herangezogen. Total wurden rund 2.6 Mio. versicherte Tage berücksichtigt, in denen total 79 Auffahrkollisionen verursacht wurden. Die Zahl der relevanten Unfälle pro versicherter Tag, also die Frequenz von Auffahrkollisionen, der beiden Fahrzeugmodelle wurde verglichen. Das Resultat: mit der Mercedes B-Klasse mit CPA wurden 69% weniger Auffahrkollisionen verursacht als mit der B-Klasse ohne CPA.

4. Retrospektive Studie zu Parksensoren

Die Auswahl der Fahrzeuge für die Untersuchung zu Parksensoren gestaltete sich nicht einfach. Es wurden die Unfälle beim Parkieren des Dacia Sanderos Modell 2008 ohne Parksensoren verglichen mit dem Peugeot 5008I Sport Pack mit Parksensoren. Die Untersuchung ergab, dass sogar mehr Unfälle mit Parksensoren geschehen als ohne. Bei der näheren Betrachtung fiel auf, dass Beschädigungen an den Peugeots vorwiegend auf den Seiten und nicht hinten, im Bereich der Parksensoren auftraten. Das ist eine Erklärung dafür, dass kein positiver Effekt für die Parksensoren nachgewiesen werden konnte. Weitere Limitationen sind auch in dieser Studie, dass unterschiedliche Modelle, welche unterschiedlich übersichtlich sind und von unterschiedlichen Fahrern gefahren werden, verglichen wurden.

IV. Neue Risiken durch automatisiertes Fahren

Die Automobilhersteller entwickeln die Fahrerassistenzsysteme weiter und kombinieren verschiedene Fahrerassistenzsysteme. Die Vereinigung der Automobilingenieure (SAE) teilt das automatisierte Fahren von Fahrerassistenzsystemen bis hin zu fahrerlosen Fahrzeugen in sechs Stufen der Automatisierung ein[3]. Aktuelle Fahrzeuge mit Fahrerassistenzsystemen werden den Level 1 und 2 zugeordnet. Ab Level 3 ist das Fahrzeug fähig gewisse Fahrstrecken ohne Fahrer zu Fahren. Der Fahrer muss aber jederzeit bereit sein, das Fahrzeug wieder zu übernehmen. Ein Fahrzeug mit Level 4 Funktionen kann gewisse Strecken fahrerlos Fahren, wobei der Fahrer nicht übernehmen können muss.

[3] SAE.

Falls der Fahrer das Fahrzeug nach Aufforderung des Fahrzeugs nicht übernimmt, kann das Fahrzeug sich selbst in einen minimal riskanten Zustand versetzen, zum Beispiel parken. Level 5 beschreibt Fahrzeuge, welche auch ohne Lenkrad auskommen können, in welchem also alle Insassen Passagiere sind. Level 5 Fahrzeuge sind fahrerlos.

1. Level 3

Gemäss einer Studie von EBP werden insbesondere mit Level 3 potentiell mehr Unfälle erwartet[4]. Die Experten erwarten insbesondere, dass die Fahrer der Technik zu stark vertrauen und dadurch Unfälle verursacht werden. Erste Unfälle, bei denen vermutet wird, dass der Fahrer sich zu stark auf die Technik verlassen hat, wurden bereits verursacht. Insbesondere Fahrzeuge, welche Fahrerassistenzsysteme zur Spurhaltung und den adaptiven Tempomaten verbinden, um auf der Autobahn oder im Stau ohne Input des Fahrers gewisse Strecken zu fahren, sind davon betroffen, die Vorstufe von Level 3.

2. Cyberrisiken

Automatisierte Fahrzeuge werden vernetzt sein. Die Vernetzung führt dazu, dass potentiell Hackerangriffe möglich sind. An den Crashtests 2017 hat die Unfallforschung & Prävention der AXA auf mögliche Hackerangriffe hingewiesen und darauf aufmerksam gemacht, wie wichtig es bereits in naher Zukunft sein wird, dass nach einem Unfall Daten zur Verfügung stehen, welche die Fahrt kurz vor dem Unfall beschreiben. Nur mit entsprechenden Daten wird es in Zukunft möglich sein, Unfälle zu rekonstruieren und die Unfallursache – zum Beispiel auch Hackerangriffe – zu eruieren.[5]

3. Herausforderung Mischverkehr

Als grosse Herausforderung wird der Mischverkehr gesehen. Auf der einen Seite der Mischverkehr der verschiedenen Automatisierungslevel. So wird ein Level 4 oder Level 5 Fahrzeug, welches in den nächsten 15 Jahren auf den Markt kommt, mutmasslich mit den Fahrzeugen, welche heute verkauft werden, die Strasse teilen müssen. Somit muss ein automatisiertes Fahrzeug mit von Menschen gelenkten Fahrzeugen interagieren können.

---

4 Willi.

5 AXA.

Aber auch der Mischverkehr der verschiedenen Verkehrsteilnehmer ist eine Herausforderung für ein automatisiertes Fahrzeug. In der Stadt muss ein automatisiertes Fahrzeug auf Fussgänger jeden Alters, auf Fahrradfahrer, auf Motorradfahrer und auf alle weiteren Verkehrsteilnehmer reagieren können.

4. Moralische Entscheidungen

Das Beispiel wirkt konstruiert, die grundsätzliche Fragestellung aber nicht. Ein automatisiertes Fahrzeug fährt in einem Tunnel mit Gegenverkehr. Ein Personenwagen kommt entgegen. Plötzlich überholt ein Quad den entgegenkommenden Personenwagen. Das automatisierte Fahrzeug bremst, kann aber nicht ausweichen und muss entweder in den entgegenkommenden Personenwagen oder in das entgegenkommenden Quad fahren. Das Fahrzeug könnte – im Gegensatz zu einem Fahrer – in Sekundenbruchteilen eine Entscheidung faktenbasiert treffen und gezielt entweder den Personenwagen oder das Quad treffen. Die Ethikkommission in Deutschland hat bereits Grundsätze für diese Fragestellung veröffentlicht. In diesem Bericht steht geschrieben:

> „*Die Programmierung ist deshalb im Rahmen des technisch Machbaren so anzulegen, im Konflikt Tier- oder Sachschäden in Kauf zu nehmen, wenn dadurch Personenschäden vermeidbar sind.*“ [6]

Doch was heisst das in diesem Fall? Es wird nicht möglich sein, zu wissen, wie verletzlich die Personen im Personenwagen sind und ob der Quadfahrer bei der Kollision Verletzungen davontragen würde. Selbst diese scheinbar einfachen Regeln wird ein System nicht in jeder Situation umsetzen können. Die aktuelle Lösung ist, dass die Fahrzeuge in der Lage sein müssen, jegliche Kollisionen zu verhindern.

V. Diskussion und Fazit

Fahrerassistenzsysteme erhöhen die Verkehrssicherheit, dies wird durch unterschiedlichste Studien nachgewiesen. Bei Personenwagen sind je nach Datengrundlage insbesondere ESP und Notbremsassistenten sehr wirksam. Die Versicherungsstatistik zeigt, dass viele Unfälle beim Parken und Manövrieren geschehen – trotz Parksensoren. Da die Beschädigungen der Verunfallten Personenwagen häufig seitlich anzutreffen sind, besteht die Möglichkeit, dass

[6] BMVI.

zukünftige, weiterentwickelte Einparkhilfen tatsächlich zu weniger Unfällen beim Parkieren führen und so die Statistik der Versicherer positiv beeinflussen.

Beim Motorrad wurde die Wirksamkeit von ABS nachgewiesen. Heute ist ABS für schwere Motorräder bereits Pflicht, doch leider für leichtere Motorräder und insbesondere für die Roller mit 50 cm3-Motoren kaum erhältlich. Da die meisten Motorradfahrer mit einem kleineren Motorrad das Fahren erlernen und das unter Umständen in jugendlichem Alter, ist diese Tatsache umso tragischer.

Mit der zunehmenden Verbreitung von Fahrerassistenzsystemen und neuen Systemen bis hin zum automatisierten Fahren der verschiedenen Level werden auch neue Risiken erwartet. Es ist anzunehmen, dass dank Sensibilisierungskampagnen auch die neuen Risiken den Strassenverkehr langfristig nicht riskanter werden lassen. Vielmehr ist die Hoffnung da, dass auch im Strassenverkehr die Übernahme der Fahraufgabe durch eine Maschine am Ende zu weniger Fehlern und damit weniger Unfällen führt.

Literatur

ASTRA, abrufbar unter: <https://www.astra.admin.ch/astra/de/home/dokumentation/unfalldaten/grundlagen/unfallerfassung.html>.

bfs, abrufbar unter: <https://www.bfs.admin.ch/bfs/de/home/statistiken/mobilitaet-verkehr/unfaelle-umweltauswirkungen/verkehrsunfaelle/strassenverkehr.html>.

SAE, SAE International, Automated Driving Levels of Driving Automation, SAE J3016.

Willi Christian et al., Automatisiertes Fahren, Auswirkungen auf die Strassenverkehrssicherheit, EBP 2018.

AXA, Autonomes Fahren – Mensch oder Maschine, Broschüre AXA Crashtests, 2017.

BMVI, Ethik-Kommission Automatisiertes und vernetztes Fahren, Bundesministerium für Verkehr und digitale Infrastruktur, Deutschland, 2017.

Digitale Kriminalität

Thomas Wenk

Inhalt

I. Einleitung

Gemäss eines Berichts der EU Kommission vom Februar 2019 sind bei der Aufklärung von mindestens 85% aller Kriminalfälle digitale Spuren und/oder digitale Beweise von Relevanz.

Kriminalität im digitalen Bereich hat in den letzten Jahrzehnten mit der zunehmenden Digitalisierung der Gesellschaft Einzug genommen.

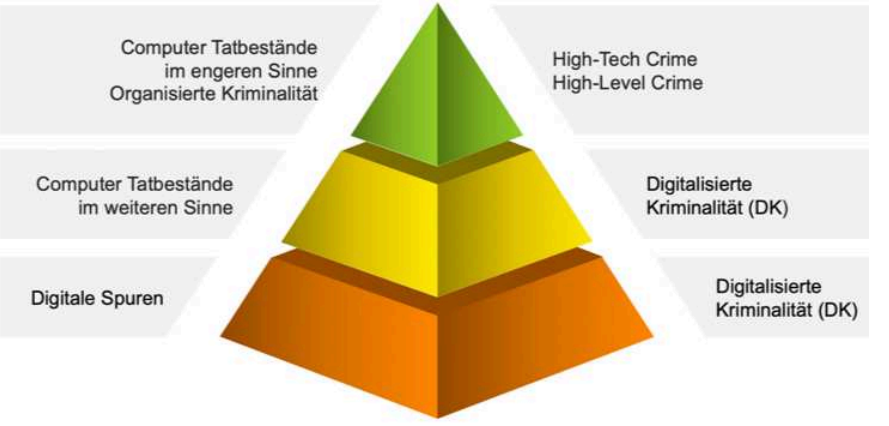
Aufgrund der relativ neuen Kriminalitätsformen werden die Begriffe und Bezeichnungen zum Teil verwechselt oder in unterschiedlichen Zusammenhängen verwendet.

Der Begriff „Cybercrime“ ist ein Beispiel für einen Begriff, welcher verschiedene Bedeutungen haben kann. Viele ausländische Polizeikorps beginnen, statt „Cybercrime“ denn Begriff „High-Tech Crime“ zu verwenden. Die Stadtpolizei Zürich verwendet neu ebenfalls diesen Begriff, jedoch um den Term „High-Level“ ergänzt, welcher darauf hinweisen soll, dass die Organisationsform der Kriminalität sich ebenfalls auf einer sehr hohen Ebene befinden kann.

Dieses Dokument soll nach aktuellem Stand (Juni 2019) die Begriffe definieren.

II. Digitale Kriminalität

1. Übersicht



2. High-Tech/High-Level Crime

Der Begriff „High-Tech/High-Level Crime" soll das sehr strapazierte Wort „Cybercrime" ersetzen.

a) Definition High-Tech Crime

In den Bereich „High-Tech Crime" fallen Delikte, welche mittels technisch sehr hochstehenden Tatwerkzeugen begangen werden und/oder mit einem grossen Mass an Technikeinsatz begangen werden.

Technisch hochstehende Tatwerkzeuge können beispielsweise ausgeklügelte, spezialisierte Computerprogramme sein, welche zum Ziel haben, kritische Infrastrukturen zu manipulieren oder zu sabotieren.

Bei einem hohen Technikeinsatz wird ein grosses Mass an Technik für die Begehung eines Deliktes verwendet. Die Qualität und Komplexität sind dabei gering, es werden jedoch mengenmässig eine sehr grosse Anzahl von diesen Massnahmen verwendet. Ein gutes Beispiel sind Denial-of-Service (DOS oder distributed DOS), welche mittels trivialer Technologie, jedoch in sehr grosser Anzahl durchgeführt werden.

In der Praxis ist meist der hohe Technikeinsatz anzutreffen; die ausgeklügelten, spezialisierten Super-Virus-Malware-Programme, wie sie in Fernsehserien zum Einsatz kommen, sind nur selten anzutreffen.

b) Definition High-Level Crime

High-Level Crime beschreibt die Organisationsform, wie die Taten begangen werden.

Folgende Eigenschaften können High-Level Crime definieren:

- staatliche Akteure
- Verteilung über mehrere Nationen, wenig oder kein Bezug zur Schweiz
- hoher Organisationsgrad der Täterschaft (Organisierte Kriminalität, etc.)

c) Massnahmen im Bereich „High-Tech/High-Level Crime"

Im Bereich von „High-Tech/High-Level Crime" sind polizeiliche Aufklärungsmassnahmen nach aktuellem Stand nur in den wenigsten Fällen aussichtsreich. Die Wirtschaftlichkeit dürfte gegen 0 tendieren. Grund dafür sind u.a. die aktuellen juristischen Hindernisse bei internationalen Verfahren, die administrativen Aufwände mit den damit verbunden Reaktionszeiten, die genutzten einfachen, aber effektiven Verschleierungsmassnahmen der Täterschaft sowie die Aufbewahrungsfristen von Metadaten.

In diesem Bereich müssen sich Behörden hauptsächlich auf präventive Massnahmen konzentrieren, um die Entstehung solcher Kriminalität gar nicht erst zuzulassen.

Zukünftig können solche Kriminalitätsformen effizient und effektiv bekämpft werden, wenn die Strafverfolgung ähnlich organisiert ist wie die Täterschaft. Dies bedingt eine reibungslose und hindernisfreie internationale Zusammenarbeit oder die Formierung einer übergreifenden internationalen Strafverfolgungsbehörde.

3. Digitalisierte Kriminalität

a) Digitalisierte Kriminalität

Unter dem Begriff der Digitalisierten Kriminalität werden althergebrachte Kriminalitätsformen zusammengefasst, welche im Rahmen der weltweiten Digitalisierung mithilfe von digitalen Tatwerkzeugen begangen werden und/oder digitale Spuren hinterlassen.

Fand früher der Betrug in der realen Welt statt, so wird dieser heute oft über digitale Inserate- und Auktionsplattformen begangen. Dabei werden Tatwerkzeuge wie Email oder eine Bezahlung mit digitalen Währungen einbezogen.

Weitere Beispiele sind:

- Erpressung aller Art (mit gestohlenen Bildern/Videos, Sextortion, via SMS, WhatsApp)
- Erwachsene, die sich im Internet gegenüber Minderjährigen als ebenfalls Minderjährige ausgeben (Grooming)
- Handel mit verbotenen Substanzen im Internet (oder Darknet)
- Handel mit verbotenen Gegenständen (z.B. Waffen) im Internet (oder Darknet)
- Üble Nachrede, Verleumdung, Rufschädigung etc. via Facebook etc.
- Konsum, Verbreitung, Herstellung von verbotener Pornografie (Art. 197 StGB)
- etc., etc.

Bei der Täterschaft handelt es sich oft um lokal ansässige Täter oder um Täter mit lokalem Bezug.

b) Digitale Spuren

Digitale Spuren entstehen heute an zahlreichen Orten. Die Auswertung kann wichtige Hinweise zur Klärung von Kriminalfällen geben; bereits vorhandene konventionelle Spuren können belegt oder widerlegt werden.

Digitale Spuren finden sich in allen elektronischen Geräten wie:

- Computern
- (Mobil-)Telefonen, Smartphones, Tablets, etc.
- Datenträgern wie Festplatten, USB Sticks, Speicherkarten
- Smart-TV's, elektronischen Türschlössern etc.
- Elektronischen Hilfsmitteln und Haushaltgeräten (Staubsauger, Kühlschränke, etc.)
- Fahrzeugen aller Art (z.B. PKW, LKW, eBikes)

Digitale Spuren und Hinweise sind ebenfalls im Internet zu finden. Sei dies auf Social Media Plattformen, wo die Daten öffentlich zur Verfügung gestellt werden, aber auch in sogenannten Cloud-Diensten wie beispielsweise Dropbox, iCloud, Google Cloud und verschiedenen Emaildiensten.

Je weiter die Digitalisierung fortschreitet, umso mehr digitale Spuren fallen an.

Wichtig ist die Feststellung, dass digitale Spuren *zusätzlich* zu den herkömmlichen Spuren anfallen.

c) Massnahmen im Bereich Digitalisierte Kriminalität

Auch in diesem Bereich ist die Prävention von grosser Bedeutung. Anders als bei High-Tech/High-Level Crime sind die Aufklärungsmöglichkeiten bei Digitalisierter Kriminalität jedoch vorhanden, da in den meisten Fällen ein starker Bezug zur realen Welt und/oder ein starker lokaler Bezug besteht.

III. National Center for Missing & Exploited Children (NCMEC)

Die Schweizer Presse hat Anfang 2019 berichtetet, dass immer mehr Fälle von verbotener Pornografie durch das FBI an die Schweizer Polizeibehörden gemeldet werden.

Diese Aussage ist nur teilweise richtig: der starke Anstieg der gemeldeten Fälle kann bei der Stadtpolizei Zürich nachvollzogen werden. Fälle dieser Art sind haben von 2015 bis 2018 um den Faktor 11 zugenommen.

Falsch ist jedoch die Aussage, dass die Fälle durch das FBI gemeldet werden.

1. Ablauf bei NCMEC-Fällen

Lädt jemand im Internet bekannte, verbotene Pornografie mit Minderjährigen hoch, so melden die Betreiber der jeweiligen Plattformen freiwillig und gemäss ihren Nutzungsbedingungen diese Verstösse an das NCMEC (National Center for Missing & Exploited Children) weiter.

Beispiele solcher Plattformen sind:

- OneDrive (Microsoft)
- iCloud (Apple)
- Google Drive (Google)
- Facebook (inkl. zugehörige Applikationen wie Instagram)

NCMEC sammelt die Daten, triagiert nach Nationen und leitet die Informationen an die jeweils zuständigen Landespolizeiorganisationen weiter. Diese übernehmen die Verteilung an die zuständigen Polizeiorganisationen.

2. Praxisbeispiel NCMEC Fall

- Upload verbotener Inhalt durch Zürcher*in auf OneDrive
- Feststellung aufgrund von Hashwerten (Prüfsummen)
- Meldung des Providers (OneDrive = Microsoft) an NCMEC
    - Hashwert der Datei
    - Datum, Zeit
    - Benutzernamen
    - IP Adressen
- Meldung von NCMEC an FEDPOL
- Meldung von FEDPOL an Stadtpolizei Zürich

Künstliche Intelligenz & Präventionsarbeit

Ulrich Schimpel

Inhalt

I. Einleitung

Das Thema Künstliche Intelligenz (KI) ist aus dem heutigen Alltag quer über alle Industrien und Gesellschaftsgruppen kaum mehr wegzudenken – obwohl der Begriff einige auch grundsätzliche Diskussionen auslöst. Zum einen fällt bereits eine saubere Abgrenzung des Begriffs schwer. Zum anderen hat die Anwendung von KI und KI-Systemen Auswirkungen weit über die Technologie selbst und deren Anwender hinaus, bis hin zu juristischen und ethischen Aspekten[1].

[1] European Commission, Ethics guidelines for trustworthy AI.

Die Europäische Kommission definiert Künstliche Intelligenz als „Systeme, die intelligentes Verhalten dadurch zeigen, dass sie ihre Umgebung analysieren und – mit einem gewissen Grad an Autonomie – handelt, um spezifische Ziele zu erreichen." [2]

Auch in der Präventionsarbeit versprechen sich die verschiedenen Akteure vom Einsatz neuer KI-Systeme oft grosse Vorteile bezüglich Qualität und Geschwindigkeit bei der Bewältigung ihrer Aufgaben.

Die folgenden Kapitel motivieren, warum neuartige Systeme benötigt werden, gehen kurz auf wissensbasierte Systeme – eine wichtige Untergruppe von KI-Systemen – ein und zeigen abschliessend einige Praxisbeispiele, Grenzen und Risiken auf.

II. Warum brauchen wir Künstliche Intelligenz und neuartige Systeme?

KI ist kein neues Phänomen, sondern hat seine Ursprünge bereits in den 1950er Jahren. Es wechselten sich Perioden grossen Optimismus mit Zeiten der Ernüchterung ab, dem sogenannten ersten und zweiten „KI-Winter", um in den letzten Jahren wieder eine Renaissance zu erfahren. Es stellt sich also die Frage, ob und warum KI und neuartige Systeme heute essentiell sein sollen, also mehr als nur ein temporäres Phänomen.

Eine der Antworten auf diese Frage ergibt sich aus der Menge, Zusammensetzung und Wachstum verfügbarer Daten, siehe Abbildung 1.

Zum einen wächst die Datenmenge aufgrund einer beschleunigten Digitalisierung und Vernetzung der Welt und einer Miniaturisierung der Geräte exponentiell auf geschätzte 175 Zettabyte[3] in 2025. Der kritische Unterschied zum bisherigen Wachstum des Datenvolumens ist die Tatsache, dass der Anteil von unstrukturierten Daten – von Multimedia bis Sensoren und deren Zeitreihen – massiv zunimmt. Traditionelle IT Systeme sind allerdings auf die Verarbeitung von strukturierten Daten optimiert und haben teilweise sehr grosse Schwierigkeiten, unstrukturierte Daten effizient und mit adäquater Geschwindigkeit zu prozessieren.

---

2 European Commission, A definition of AI.

3 1 Zettabyte = 1'000'000'000 Terrabyte.

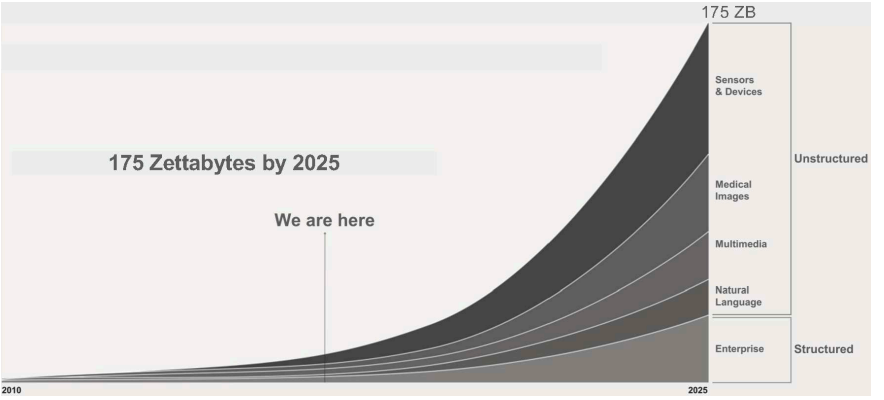


Abbildung 1: Prognose zu Datenwachstum und -struktur[4].

Daraus ergibt sich das Problem, Erkenntnisse aus den riesigen verfügbaren Datenmengen zu extrahieren. Man spricht hier auch von „dark data", also Daten, die sich einer weiteren Verwendung komplett entziehen. Einige Schätzungen gehen davon aus, dass bis zu 80% der aktuellen Daten nicht genutzt werden bzw. genutzt werden können. Dieser Prozentsatz droht sich mit dem exponentiellen Wachstum unstrukturierter Daten noch zu erhöhen, mit signifikanten Auswirkungen auf eine informierte Entscheidungsfindung durch die verantwortlichen Personen gerade bei komplexen Aufgabenstellungen.

Es besteht also ein erheblicher Bedarf an neuartigen technischen Verfahren und (Computer-) Systemen, um die Masse vor allem an unstrukturierten Daten effizient und schnell verarbeiten zu können. Nur so ist es möglich, die wachsende Menge an Daten nicht nur zu speichern, sondern auch nutzenstiftend für Entscheidungen einzusetzen.

1. Lernverfahren und Elemente der KI

Ein aktuell sehr prominenter Vertreter technischer Verfahren sind Neuronale Netze und „Deep Learning". Es existiert aber eine weit grössere Vielfalt technischer (Lern-) Verfahren, die bei der Realisierung „künstlich intelligenter" Systeme zur Anwendung kommen. „Maschinelles Lernen" lässt sich beispielsweise in überwachte, nicht überwachte und sich verstärkende (reinforced) Lernal-

[4] IBM Prognose basierend auf IDC Bericht.

gorithmen unterteilen, die jeweils eine mathematische Formel generieren, um aus vorhanden Daten eine Entscheidung zu berechnen[5] – so auch Neuronale Netze.

Meist bestehen KI-Systeme aus einer Vielzahl verschiedener Elemente, die zur Ausführung bestimmter Aufgaben wie Sprach- und Bilderkennung, Problemlösung, logisches Schliessen, Wissensrepräsentation und Vorhersagen optimiert und kombiniert werden[6].

Heute sind KI-Systeme in der Lage, Spiele und Quizshows gegen die besten menschlichen Spieler zu gewinnen und sogar Debatten zu führen[7]. Ein grosses Problem bei der industriellen Anwendung und Akzeptanz von KI-Systemen, gerade bei wichtigen und komplexen Fragestellungen, stellt die Erklärbarkeit dar. Darunter versteht man die Fähigkeit des KI-Systems, dem Anwender und Entscheider die Gründe für das berechnete Ergebnis erläutern zu können. Gerade Verfahren wie das „Deep Learning" haben hier beträchtliche Schwierigkeiten, auch wenn verstärkt Forschungsarbeit in diesem Bereich getätigt wird. Fehlt diese Erklärkomponente, spricht man gerne auch von einer „black box". Systeme mit einer Erklärkomponente werden dagegen oft als Expertensysteme oder wissensbasierte Systeme bezeichnet, was nicht ausschliesst, dass auch sie „black box" Komponenten für die Bearbeitung oder Lösung von Teilaufgaben verwenden.

Der Grossteil dieser Publikation bezieht sich auf wissensbasierte Systeme, die ihren Dienst oft als Entscheidungsunterstützung für Experten bei der Durchführung zum Teil höchst anspruchsvoller Arbeiten leisten. Darunter fällt auch die Polizei- und Präventionsarbeit.

2. Neuartige Systeme und nicht-deterministische Ergebnisse

Der Fortschritt der technischen Lernverfahren hängt eng mit der Entwicklung neuer (Computer-) Systeme und „Hardware" zusammen. Prominente Vertreter sind hier Verfahren, die sich das menschliche Gehirn als Vorbild nehmen, da dieses für die Leistungserbringung sehr viel weniger Energie verbraucht als aktuelle Computer.

Weitere neuartige Ansätze sind Quantencomputer[8] und die Verwendung von „widerstandsbasierten Arbeitsspeichern"[9]. Ohne in weitere Details zu gehen

5 European Commission, A definition of AI, 3.

6 Bitkom, Periodensystem der Künstlichen Intelligenz.

7 Gabbatt, Watson wins Jeopardy clash; Teich, IBM Project Debater.

8 IBM Research, Quantum Computing.

9 IBM Research, Hardware für Künstliche Intelligenz; Gallo et al.

– der interessierte Leser sei an die angegebene Literatur verwiesen – haben diese neuartigen Systeme ebenso wie die KI-Systeme einen entscheidenden Unterschied zu den gewohnten Resultaten vieler aktueller Anwendungen: die Resultate sind nicht deterministisch. Es gibt also kein „richtig“ oder „falsch“, sondern die Ergebnisse unterliegen alle einer gewissen Wahrscheinlichkeit, wie beispielsweise auch Wetterberichte.

Ein Ergebnis ist also mit einer gewissen Wahrscheinlichkeit und Konfidenz richtig (und falsch). Der Anwender von KI-Systemen muss sich dieser Tatsache bewusst sein, ebenso wie die Darstellung von KI-Ergebnissen diesem Sachverhalt Rechnung tragen muss – neben der weiterhin notwendigen Benutzerfreundlichkeit. Daraus lässt sich ein erheblicher Ausbildungs- und Übungsbedarf für zukünftige Anwender und Entscheider ableiten, um nicht nur eine falsche Verwendung von KI-Systemen zu vermeiden, sondern vielmehr auch ihr volles Potential ausschöpfen zu können.

III. Was sind wissensbasierte Systeme?

Wissensbasierte Systeme werden auch Expertensysteme genannt, sind eine Untergruppe von KI-Systemen und zeichnen sich durch die explizite Repräsentation ihres Wissens aus. Dies ermöglicht die, für viele Bereiche der Polizei- und Präventionsarbeit essentielle Funktionalität der Erklärbarkeit berechneter Ergebnisse – im Gegensatz zum „black box“ Ansatz, wie in Kapitel II erläutert. Moderne wissensbasierte Systeme folgen einem ähnlichen Aufbau, siehe Abbildung 2.

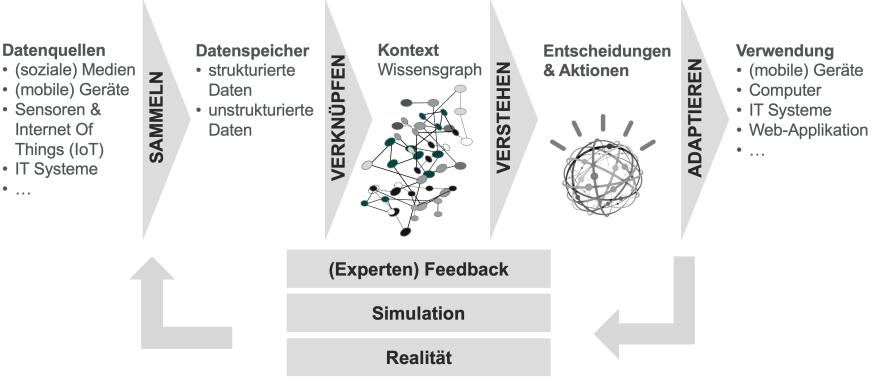


Abbildung 2: Stereotypischer Aufbau „wissensbasierter Systeme“.

1. Daten sammeln

Strukturierte und unstrukturierte Daten verschiedensten Ursprungs und unterschiedlicher Aggregation werden in der Datenbasis des wissensbasierten Systems gespeichert. Dabei ist „mehr“ nicht immer „besser“. Ein besonderes Augenmerk liegt in der Auswahl relevanter und qualitativ hochwertiger Daten. Oftmals ist es ratsam, sich an den Datenquellen der menschlichen Experten zu orientieren und diese bei Bedarf gezielt zu erweitern.

2. Daten verknüpfen

Im Zentrum jedes wissensbasierten Systems steht ein Wissensgraph, die zentrale Komponente für seine Erklärbarkeitsfunktion. Eine Hauptaufgabe und grosse Herausforderung stellt das Erarbeiten aller relevanten Verknüpfungen zwischen den unterschiedlichen Daten dar. Es reicht dabei bei weitem nicht aus, nur Synonyme oder Schlüsselwörter zu finden. Vielmehr geht es darum, die relevanten Objekte und Zusammenhänge in den (un-)strukturierten Daten zu erkennen, siehe Beispiel in Abbildung 3.

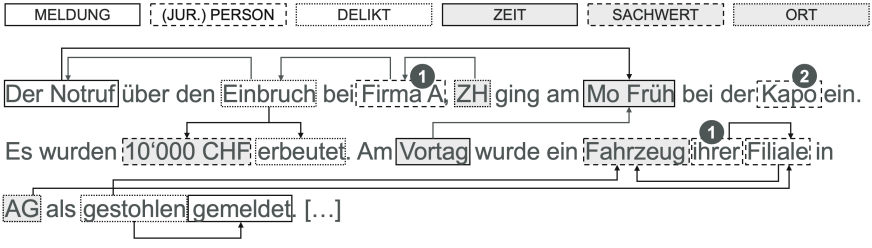


Abbildung 3: Beispielhafte Analyse relevanter Textelemente und deren Beziehung.

Auch hier empfiehlt es sich, auf Basis existierenden Expertenwissens die relevanten Objekte, Sachverhalte und Beziehungen zu erarbeiten, und in einem iterativen Vorgehen, zusammen mit den Experten, kontinuierlich zu verbessern.

Es wird offensichtlich, dass diese Aufgabe nur möglich ist, wenn eine klare Abgrenzung und Definition des Anwendungsbereichs (Domäne) existiert. Ebenso wird ersichtlich, dass eine Übertragung eines Wissensgraphen von einer Domäne auf eine andere Domäne in der Regel nicht trivial ist.

Alle Verknüpfungen, implizite und explizite Regeln und andere „Meta-Daten“ werden wiederum als Daten abgespeichert und können Teil weiterer Verknüpfungen werden. Je umfangreicher und je hochwertiger die Verknüpfun-

gen eines Wissensgraphen sind, desto wertvollere und umfangreichere (Such-) Abfragen und andere Operationen können auf dem Wissensgraph gemacht werden und liefern die notwendige Substanz, um komplexe Sachverhalte adäquat zu verstehen.

3. Zusammenhänge verstehen

Zur Lösung eines aktuellen Sachverhaltes, greift man auf den Wissensgraph und all seine Verknüpfungen („offline“ Daten) zurück. Zusammen mit dem aktuellen Erkenntnisstand („real-time“ Daten) wird versucht, unter Verwendung verschiedener Methoden wie Logik, Statistik, Optimierung, wissenschaftlicher Erkenntnisse oder Prognoseverfahren eine Aussage oder Entscheidung zum aktuellen Sachverhalt zu treffen, siehe Abbildung 4. In diesem Prozess werden oft auch zusätzliche Informationen von den Anwendern erfragt, um die Wahrscheinlichkeit und Konfidenz der Aussagen des Systems zu erhöhen.

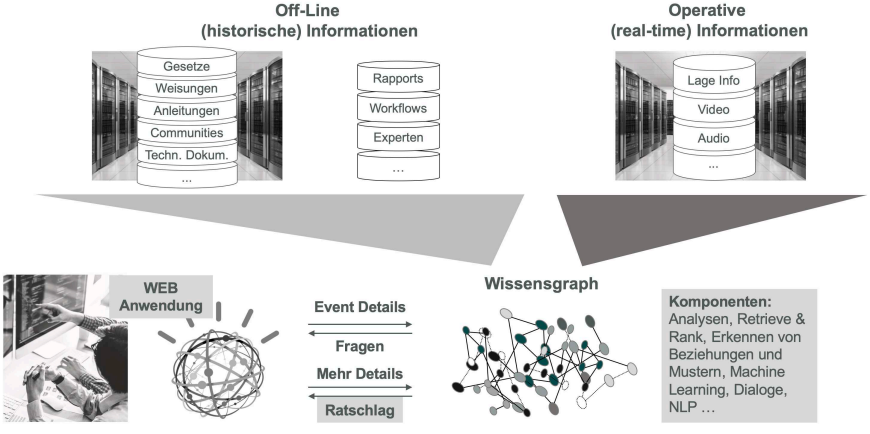


Abbildung 4: Beispielhafte Anwendung eines „wissensbasierten Systems“.

4. Aussagen und Entscheidungen kommunizieren

Eine besondere Herausforderung bei der Kommunikation zwischen einem wissensbasierten System und den verschiedenen Anwendern ist die adäquate Aufbereitung des komplexen Sachverhaltes und dessen stochastische Natur (Wahrscheinlichkeit und Konfidenz).

5. Kontinuierlich lernen

Die Präventionsarbeit agiert in einem sehr dynamischen Umfeld, wie praktisch alle komplexen Einsatzgebiete von KI-Systemen. Daraus ergibt sich die zentrale Anforderung, dass wissensbasierte Systeme (kontinuierlich) lernen müssen. Dies geschieht durch systematische und kontinuierliche Rückmeldungen, auch „feedback-loop" genannt. Je nach Situation erfolgt die Rückmeldungen üblicherweise durch …

- einen Experten oder Entscheider, der den Vorschlag des wissensbasierten Systems korrigiert – im besten Fall unter Angabe der ausschlaggebenden Aspekte.
- das Ergebnis einer (realen) Simulation.
- das Abwarten der Geschehnisse in der Realität.

In jedem Fall liefern die Rückmeldungen wertvolle Informationen und Einblicke, die wiederum in der Datenbasis des wissensbasierten Systems gespeichert, und zur Verbesserung des Wissensgraphen verwendet werden. Unter Umständen kann das Feedback auch darauf hinweisen, dass neue Datenquellen oder Elemente für die adäquate Weiterentwicklung des wissensbasierten Systems und seines Wissensgraphen notwendig sind.

IV. Praxisbeispiele

KI-Systeme werden bereits heute in verschiedenen Bereichen der Präventionsarbeit verwendet, deren Bandbreite anhand nachfolgender Beispiele aufgezeigt werden soll.

1. Proaktive Polizeiprävention

Im Jahr 2015 stehen die Polizeikräfte von Manchester, NH, USA (MPD) vor der grossen Herausforderung, trotz reduziertem Personal der stark wachsenden Kriminalität im Zusammenhang mit der dort herrschenden „Heroin Epidemie" Einhalt zu gebieten[10]. Erste Versuche mit händischen Risikoanalysen anhand historischer Daten und Trends sind aufgrund der schwerfälligen und reaktiven Natur der Prozesse und des gesamten Projektes gescheitert. Es fehlen vor allem Echtzeitdaten und zuverlässige Prognosen, um proaktiv in Gebieten tätig zu werden, in denen die Wahrscheinlichkeit für bevorstehende kriminelle Aktivitäten hoch ist.

[10] IBM, Manchaster Police Department.

Durch das Auswerten relevanter (Echtzeit-) Daten, ihrer Verknüpfung mit wissenschaftlichen Modellen zur Entstehung und Entwicklung von Kriminalität und einer schnellen (Neu-) Berechnung der Ergebnisse gelingt es MPD, signifikante Erfolge zu erzielen:

- Reduktion der Raubüberfälle um 28% binnen eines Jahres.
- Reduktion der Einbrüche um 17% binnen eines Jahres.
- Reduktion der Fahrzeugdiebstähle um 36% binnen eines Jahres und sogar um 43% auf Basis des 20-Wochen-Trends vor Einführung des neuen Polizeisystems.

Ausserdem gelingt es MPD, von einem retrospektiven „hotspot policing" zu einem prognostizierenden Einsatz der Polizeikräfte überzugehen, das sogenannte „predictive policing" beziehungsweise das weiterentwickelte „intelligence-led policing". Basierend auf den Modellen können präzisere Aussagen zu „Wer?", „Was?", „Wann?" und „Wo?" gemacht werden. Ebenfalls lernen die Polizeikräfte kontinuierlich neue Einflussfaktoren, die für die effektive und effiziente Prävention von Kriminalität genutzt werden können.

Es gibt zwei weitere interessante und wichtige Aspekte. Zum einen wurde ein kooperatives und agiles Vorgehen gewählt, um das System in einem ersten „proof-of-concept" zu validieren und in enger Zusammenarbeit mit den (Polizei-) Experten von Anfang an und über die gesamte Zeit hinweg kontinuierlich zu verbessern. Zum anderen ermöglichen die gezielte, proaktive Präsenz und ein geringerer manueller Analyseaufwand einen verbesserten persönlichen Kontakt zwischen Polizei und der Bevölkerung.

2. Risikoprognosen für die Ausbeutung von Kindern durch Banden

Die Bezirke Brent und Essex in UK setzen gezielt Prognose-Systeme ein, um verschiedene Risiken für Kinder besser einschätzen zu können, beispielsweise dass sie von Banden ausgenutzt werden oder für den Grundschuleintritt nicht adäquat vorbereitet sind[11].

Mittels vorhandener pseudonymisierter Daten werden Profile zu Kindern in einem Stadtteil erstellt, um diese auf die Kinder weiterer Stadtteile anzuwenden und zu identifizieren, welche von ihnen beispielsweise weder ausreichend Lesen noch Schreiben können. Ein weiteres Bestreben ist, die Schulreife von Kindern in kritischen Regionen – teilweise mit einem Anteil von 25% an schulunreifen fünfjährigen Kindern – gezielt zu verbessern. So konnten in einer

11 McIntyre/Pegg.

Analyse 511 Haushalte in Vange mit „gefährdeten" Kindern identifiziert werden, von denen 280 Haushalte den zuständigen Behörden und Organisationen noch nicht bekannt waren.

In anderen Bereichen wurden relevante pseudonymisierte Daten von Schulen, Sozialarbeit und Berichte zu Bandenaktivitäten und Jugendkriminalität zusammengeführt, um mittels KI-Verfahren zu identifizieren, welche Kinder einer akuten Gefahr von krimineller Ausbeutung ausgesetzt sind – um präventiv intervenieren zu können. Ähnliche Anstrengungen wurden unternommen, um zu intervenieren, bevor Kinder den Sozialbehörden überstellt werden müssen.

Die Bezirke Brent und Essex nennen als Priorität für den Einsatz von KI-Systemen die Bereiche „Banden", „sexuelle Ausbeutung von Kindern", „Vermisstensuche", „Bildung" und „Jugendkriminalität". Die KI-Systeme werden dabei zur Entscheidungsunterstützung der verantwortlichen Personen verwendet und nicht, um existierende Verantwortlichkeiten und Entscheidungsprozesse zu ersetzen.

Diese Beispiele zeigen einerseits das grosse Potential von KI-Systemen in der Präventionsarbeit und gleichzeitig auch die enge Verknüpfung zwischen der Anwendung von KI-Systemen mit essentiellen Fragestellungen bezüglich Datenschutz, Entscheidungskompetenz sowie gesellschaftspolitischen und ethischen Aspekten.

3. Erkenntnisse zur Rekrutierung bei organisiertem Verbrechen und Terrorismus

Das EU H2020 Projekt PROTON[12] widmet sich der Aufgabe, existierendes Wissen über die Rekrutierungsprozesse bei Netzwerken organisierter Kriminalität und Terrorismus zu erweitern. Dazu kombinieren die Partner Verfahren der Sozialwissenschaften und technischer Wissenschaften inklusive KI-Verfahren.

Ein zentraler Aspekt ist das Erstellen von Profilen und Laufbahnen (zukünftiger) Rekruten, Anwerber und Propagandisten. Dabei werden neben den „traditionellen" kriminellen Netzwerken für Drogen-, Menschen- und Wildtierhandel auch die Aktivitäten krimineller Cyber-Netzwerke bezüglich Rekrutierung, Werbung und Ausführung von Straftaten analysiert.

Ein Teil der Daten stammt von Sozialen Medien wie Twitter, Youtube und Facebook[13]. Auch Daten des sogenannten „Darknet" fliessen in die Auswer-

12 PROTON, <https://www.projectproton.eu/>

13 Rilling et al.

tungen ein. Zur Erstellung von Persönlichkeitsprofilen analysieren KI-Verfahren die publizierten Textbeiträge und leiten die Charakteristika folgender drei Persönlichkeitsmodelle ab[14]:

- Big Five
- Bedürnisse (Needs)
- Werte (Values)

Es ist sowohl möglich, das Profil einzelner Individuen zu erstellen als auch das von „Durchschnittsmitgliedern" einer bestimmten sozialen Plattform oder „Community". Natürlich unterliegen diese Analysen bestimmten Annahmen, wie beispielsweise, dass die Texte von den Autoren selbst ausgewählt und geschrieben wurden.

Auch in diesem Praxisbeispiel wird deutlich, dass die neuartigen (KI-) Verfahren vielmehr als Entscheidungsunterstützung für Experten dienen, als dass sie Entscheidungen und komplette Prozesse automatisieren.

4. Intelligente Audio- und Videoanalyse

Ein sehr bekannter Einsatz von KI-Verfahren in der Präventions- und Polizeiarbeit ist die Video- und Audioüberwachung. Gerade im öffentlichen Raum kann eine intelligente Kombination von Audio- und Videoanalyse sehr wertvoll sein[15]. So sind quietschende Reifen oder ein erhöhter aggressiver Lärmpegel hochwertige Indikatoren für eine potentiell gefährliche Situation. Kombiniert mit einer Videoanalyse können Situationen so schneller und treffsicherer eingeschätzt werden.

Neben dem Erkennen von Schlüsselwörtern bei der Audioanalyse oder kritischen Lärmcharakteristika lassen sich Emotionen auch in einem hohen Grad aus einer Analyse des gesprochenen (oder geschriebenen) Textes ableiten[16].

Bei der intelligenten Videoüberwachung sind viele Städte und Staaten bereits weit fortgeschritten. Dies geht bis zu grossangelegten Projekten wie „Sharp Eyes"[17] in China, welches Fehlverhalten (im Strassenverkehr) automatisch anhand verschiedener Parameter wie Trajektorien automatisch identifiziert – ebenso wie die involvierten Personen mittels Verfahren der Gesichtserkennung und Mobilfunkortung.

---

14 IBM, Personality Insights Science; IBM, Personality Insights Models.

15 Security Today.

16 McConville.

17 South China Morning Post.

Das „Sharp Eyes“ System wird ebenfalls zur Bekämpfung von (Klein-) Kriminalität eingesetzt und basiert auf dem Prinzip des „public shaming“, bei dem die Personen mit Fehlverhalten öffentlich ausgerufen werden. Die Ideen gehen dabei weiter bis hin zur Kombination mit einem „Sozialpunktekonto“, das „schlechten“ Bürgen Reisetätigkeiten, Zutritt zu Luxushotels oder sogar Zugang deren Kindern zu guten Schulen verwehrt.

Auch dieses Praxisbeispiel zeigt, wie eng Chancen und weitreichende Auswirkungen quer durch verschiedenste Lebensbereiche bei der Anwendung von KI-Systemen verbunden sind.

V. Grenzen und Risiken

Jede Technologie und deren Anwendung hat gewisse Grenzen und Risiken. Allerdings ergeben sich bei KI durch die Lernfähigkeit, die Kombination verschiedenster Verfahren, die hohe Konzentration von personenbezogenen Daten quer über alle Lebensbereiche, deren selbstverstärkende Spirale von Skaleneffekten und durch den hohen Grad möglicher (Halb-) Automation in teilweise hoch komplexen Situationen besondere Grenzen und Risiken. Gerade bei der (präventiven) Polizeiarbeit können die Auswirkungen für betroffene Individuen gravierend sein, was zu besonderer Vorsicht und Qualitätssicherung bei den Gesamtprozessen und deren Beteiligten drängt.

1. Manipulation und Befangenheit

Insbesondere Verfahren der KI ohne Erklärkomponente – sogenannte „black box“ Verfahren – wie die meisten Neuronalen Netze, sind anfällig für unentdeckte Manipulationen (sowohl gezielte als auch unbewusste), da dem Anwender oder einer Revisionsstelle die Gründe für ihre Entscheidung nicht dargelegt werden können. Die Manipulation kann sowohl durch – für menschliche Sinne unsichtbare – Abweichungen der Daten zu einem aktuellen Sachverhalt entstehen als auch durch eine schlechte Datenbasis, um das KI-System zu trainieren.

Ein einfaches und anschauliches Beispiel sind verzerrte Bilder von Verkehrsschildern, die komplett falsch interpretiert werden. Aber auch das gänzliche Fehlen oder Ignorieren von Daten einer bestimmten Personengruppe beim Betrieb eines KI-Systems für polizeiliche Präventivmassnahmen kann bei ebensolchen Personengruppen zu beliebigen (Fehl-) Einschätzungen führen.

Aus diesen Gründen widmen sich einige aktuelle Anstrengungen der Entwicklung von Verfahren, die eine systematische Manipulation und Befangenheit möglichst ausschliessen[18].

Auch wissensbasierte Systeme unterliegen dem Risiko von Manipulation und Befangenheit. Der signifikante Unterschied liegt darin, dass die Herleitung fragwürdiger Aussagen und Entscheidungen dem Anwender oder einer Revisionsstelle bis ins Detail offengelegt werden können. Dies erlaubt eine frühzeitige und direkte Entdeckung von Defiziten und deren Behebung.

2. KI, bewährte Praxis und Ethik

Aus den genannten Risiken und deren potentiell schwerwiegenden Auswirkungen formiert sich das interdisziplinäre und organisationsübergreifende Bedürfnis, sowohl grundsätzliche Fragen zu diskutieren und beantworten als auch optimale Vorgehensweisen für den Einsatz von KI-Systemen zu erarbeiten.

Die „Partnership on AI" setzt es sich beispielsweise zum Ziel, eine optimale Praxis für ethische KI zu definieren und mit der Anwendung von KI die menschliche Intelligenz zu unterstützen, anstatt sie zu ersetzen[19]. Dabei spielen Themen wie die Transparenz eine wichtige Rolle, sowohl bezüglich dem „Wann", „Wo" und „Warum" KI-Systeme eingesetzt werden als auch bezüglich verwendeter Daten und Verfahren.

Auch auf europäischer Ebene befasst sich eine Kommission mit dem Thema „ethische Richtlinien für eine vertrauenswürdige KI".[20]

Die Diskussionen sind noch relativ jung und fern einer abschliessenden Beurteilung – sofern dies bei einer so weitreichenden, komplexen und sich rasant entwickelnden Technologie überhaupt jemals der Fall sein kann. Eine Beurteilung hängt auch teilweise vom Wertesystem der jeweiligen Gesellschaft ab und bedarf einer breiten öffentlichen Diskussion und Auseinandersetzung mit diesem Thema.

3. Mensch und Technologie

Nicht nur aus ethischen und gesellschaftlichen Gründen spricht einiges gegen das Ersetzen von menschlicher Intelligenz durch KI.

---

18 Kleinman.

19 Partnership on AI, <https://www.partnershiponai.org/>.

20 European Commission, Ethics Guidelines for Trustworthy AI.

Die aktuelle Technologie inklusive KI-Systeme haben signifikante Vorteile gegenüber dem Menschen gerade bei der Geschwindigkeit, Ausdauer und Skalierbarkeit, grosse Datenmengen zu analysieren. Weitere Vorteile sind ein „perfektes Gedächtnis" und das zuverlässige Ausführen komplizierter Rechenoperationen.

Die Vorteile des Menschen liegen hingegen im abstrakten und kritischen Denkvermögen, dem „gesunden Menschenverstand", der Intuition, Empathie und der Kreativität – und zwar quer über unterschiedlichste (Lebens-) Bereiche hinweg. Hier dürften die Menschen auch in absehbarer Zeit der KI und anderen Technologien weit überlegen bleiben.

Im Einklang mit den Diskussionen zu KI und Ethik, ist das angestrebte Ziel weiterhin eine Symbiose zwischen Mensch und Technologie, um Menschen beispielsweise mehr Zeit zur Bewältigung all jener (komplexen) Aufgaben zu geben, die eine Anwendung menschlicher Stärken bedingen.

VI. Zusammenfassung

Bereits heute eignen sich KI-Systeme für den Einsatz bei der (polizeilichen) Präventionsarbeit. Dies stellt kein Luxus dar, sondern wir benötigen KI und neuartige Systeme, um das massive Wachstum an (un-) strukturierten Daten nicht nur bewältigen zu können, sondern vielmehr, um relevante Erkenntnisse in nützlicher Frist für notwendige Entscheidungen verwenden zu können.

Sowohl „black box" Verfahren ohne Erklärkomponente als auch wissensbasierte Systeme mit einer Erklärbarkomponente sind dem Risiko einer bewussten oder unbewussten Manipulation und Befangenheit ausgesetzt. Deshalb sind Massnahmen zur Qualitätssicherung vor allen in kritischen Anwendungsbereichen der Präventionsarbeit essentiell. Dabei bedarf es einer besonderen Sensibilisierung zukünftiger Anwender mit dem Umgang von nichtdeterministischen Ergebnissen und Aussagen von KI-Systemen.

Nicht zuletzt stellen sich komplexe grundlegende, ethische und gesellschaftspolitische Fragen bei der Anwendung von KI-Systemen, die einer kontinuierlichen und breiten Diskussion bedürfen. Das primäre Ziel bei der Entwicklung von KI Systemen ist eine Symbiose von Mensch und Technologie – und nicht die Ersetzung der menschlichen Intelligenz.

Literaturverzeichnis

BITKOM (Hrsg.), Digitalisierung gestalten mit dem Periodensystem der Künstlichen Intelligenz. Berlin 2018.

European Commission (Hrsg.), Ethics guidelines for trustworthy AI, Brüssel 2019.

European Commission (Hrsg.), A definition of AI: Main capabilities and disciplines, Seite 3, Brüssel 2019.

GABBATT ADAM, IBM computer Watson wins Jeopardy clash. The Guardian, 2011, <https://www.theguardian.com/technology/2011/feb/17/ibm-computer-watson-wins-jeopardy>.

LE GALLO M. et al., Compressed sensing recovery using computational memory. 2017 IEEE International Electron Devices Meeting (IEDM), IEEE, Dezember 2017.

IBM (Hrsg.), Manchester Police Department. <https://mediacenter.ibm.com/media/Manchester+Police+Department+uses+predictive+policing+for+proactive+crime+prevention/1_vtgxpcif, https://www.youtube.com/watch?v=BNeMoIbEgI8>.

IBM (Hrsg.), Personality Insights Models, <https://cloud.ibm.com/docs/services/personality-insights?topic=personality-insights-models>.

IBM (Hrsg.), Personality Insights Sience, <https://cloud.ibm.com/docs/services/personality-insights?topic=personality-insights-science>.

IBM Research (Hrsg.), Quantum Computing, <https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/>.

IBM Research (Hrsg.), Hardware for AI, <http://www.research.ibm.com/artificial-intelligence/hardware/>.

KLEINMAN ZOE, IBM launches tool aimed at detecting AI bias, BBC, 19. September 2018.

MCCONVILLE ANTON, Measuring emotion with IBM Watson Speech to Text and Tone Analysis. IBM, 22. November 2016, <https://www.ibm.com/cloud/blog/measuring-emotion-ibm-watson-speech-text-tone-analysis>.

MCINTYRE NIAMH/PEGG DAVID, Data on thousands of children used to predict risk of gang exploitation, The Guardian, 17. September 2018.

REINSEL DAVID/GANTZ JOHN/RYDNING JOHN, The Digitization of the World – From Edge to Core, IDC White Paper, #US44413318, November 2018.

RILLING et al., Report on OC and terrorism in Cyberspace. 2018. PROTON, <https://www.projectproton.eu/wp-content/uploads/2018/01/Deliverable-D3.1.pdf>.

Security Today (Hrsg.), A sound solution in safe cities, 30. November 2016.

South China Morning Post (Hrsg.), China's Sharp Eyes surveillance system puts the security focus on public shaming, 30. Oktober 2018.

TEICH PAUL, IBM Project Debater is in the uncanny valley and why that is groundbreaking. Forbes, 7. März 2019.

Publikationsliste

letzte erschienene Bände bei EIZ Publishing, Zürich

Band 201 **Challenges, risks and threats for security in Europe**
11th Network Europe Conference, Warshaw, 19th–22nd May 2019
Andreas Kellerhals / Tobias Baumgartner (Hrsg.), mit Beiträgen von Viorel Cibotaru, Attila Vincze, Przemyslaw Saganek, Jelena Ceranic, Aleksei V. Dolzhikov, Alena F. Douhan, Darina Dvornichenko, Vadym Barskyy, Itay Fischhendler, Verena Murschetz, Jürgen Scheffran, Tobias Baumgartner, 2019 – CHF 49.90.–

letzte erschienene Bände bei Schulthess Juristische Medien AG, Zürich

Stand Dezember 2019

Band 187 **Bedrohungsmanagement – Häusliche Gewalt**
Christian Schwarzenegger / Reinhard Brunner (Hrsg.), mit Beiträgen von Jérôme Endrass, Karin Greuter, Christoph Lerch, Mike Mottl, Astrid Rossegger, Daniel Schlüsselberger, Aline Schwarz, Ilona Swoboda, 2018 – CHF 68.–

Band 188 **Kapitalmarkt – Recht und Transaktionen XIII**
Thomas U. Reutter / Thomas Werlen (Hrsg.), mit Beiträgen von David Borer, Dorothee Fischer-Appelt, Theodor Härtsch, Stefan Kramer, Lorenzo Olgiati, Matthias Portmann, Thomas U. Reutter, Olivier Thormann, Annette Weber, 2019 – CHF 78.–

Band 189 **Die Schweiz und Europa**
Referate zu Fragen der Zukunft Europas 2017
Andreas Kellerhals (Hrsg.), mit Beiträgen von Paddy Ashdown, Alain Berset, Jürg Bischoff, Martin Dahinden, Joachim Gauck, Mario Greco, André Holenstein, Stephan Husy, Mouhanad Khorchide, Roland Koch, Enrico Letta, Kishore Mahbubani, Mark Pieth, Michael Russel, 2018 – CHF 78.–

Band 190 **Private Equity VI**
PE 6.0: Neue Mitspieler, neue Technologien, neue Themen, neues Recht
Dieter Gericke (Hrsg.), mit Beiträgen von Martin Frey, Dieter Gericke, Petra Hanselmann, Margrit Marti, Luka Müller-Studer, Daniel Oehri, Rolf Sethe, Claudia Suter, Sarah Vettiger, Christian Wenger, Michelle Wiki, 2018 – CHF 78.–

Band 191 **Kurzer Prozess, zu kurzer Prozess – im Wirtschaftsstrafverfahren**
10. Schweizerische Tagung zum Wirtschaftsstrafrecht
Jürg-Beat Ackermann / Marianne Hilf (Hrsg.), mit Beiträgen von Jürg-Beat Ackermann, Christina Galeazzi, Christopher Geth, Damian K. Graf, Konrad Jeker, Michael Lauber, Barbara Lips-Amsler, Alexander Medved, Peter Pellegrini, Matthias Portmann, Nora Scheidegger, Reto Weilenmann, 2019 – 78.–

Band 192 **Sanierung und Insolvenz von Unternehmen IX**
Neue Entwicklungen
Thomas Sprecher (Hrsg.), mit Beiträgen von Lukas Glanzmann, Christian Hachmann, Daniel Hunkeler, Michel Kähr, Oliver Kälin, Benedikt Maurenbrecher, Urs Meier, Zeno Schönmann, Markus Wolf,
2019 – 69.–

Band 193 **Mergers & Acquisitions XXI**
Hans-Jakob Diem (Hrsg.), mit Beiträgen von Philipp Candreia, Hans-Jakob Diem, Dieter Gericke, Urs P. Gnos, Astrid Waser, Philippe A. Weber, 2019 – CHF 75.–

Band 194 **Beste Stiftungsratspraxis**
Welche Aufsicht haben und welche brauchen wir?
Beate Eckhardt / Thomas Sprecher (Hrsg.), mit Beiträgen von Martin Grichting, Harold Grüninger, Dominique Jakob, Thomas Ritter, Christina Ruggli-Wüest, Georg von Schnurbein, Goran Studen, 2019 – CHF 68.–

Band 195 **Bedrohungsmanagement**
Radikalisierung und gewalttätiger Extremismus/Nationaler Aktionsplan
Christian Schwarzenegger / Reinhard Brunner (Hrsg.), mit Beiträgen von Dirk Baier, René Bühler, André Duvillard, Verena Fabris, Thomas Gerber, Norbert Leygraf, Patrik Manzoni, Colette Marti,
2019 – CHF 58.–

Band 196 **Kapitalmarkt – Recht und Transaktionen XIV**
Thomas U. Reutter / Thomas Werlen (Hrsg.) – mit Beiträgen von Matthias Courvoisier, Alexander von Jeinsen, Peter Probst, Lorenzo Togni, 2019 – CHF 69.–

Band 197 **Europa in der Welt**
Referate zu Fragen der Zukunft Europas 2018
Andreas Kellerhals (Hrsg.), mit Beiträgen von Samuel Alito, Ami Ayalon, Christine Beerli, John Bercow, Ignazio Cassis, Andrzej Duda, Wolfgang Ernst, Jacqueline Fehr, Thomas Greminger, Etsuro Honda, Elke König, Andreas Lehmann, Eric LeVine, Suzi LeVine, Robert Menasse, Federico Rampini, Martin Walker, Geng Wenbing, Diane P. Wood, 2019 – CHF 79.–

Band 198 **Sanierung und Insolvenz von Unternehmen X**
Thomas Sprecher (Hrsg.), in Vorbereitung

Band 199 **Merger & Acquisitions XXII**
Hans-Jakob Diem (Hrsg.), in Vorbereitung

Band 200 **Europa als die Schweiz der Welt?**
Referate zu Fragen der Zukunft Europas 2019
Andreas Kellerhals (Hrsg.), in Vorbereitung

Ausserdem erschienen:
Bilaterale Verträge I & II – Schweiz – EU – Handbuch
Daniel Thurer / Rolf H. Weber / Wolfgang Portmann / Andreas Kellerhals (Hrsg.), mit Beiträgen von: Tobias Baumgartner, Giovanni Biaggini, Frédéric Berthoud, Theodor Bühler, Adelheid Bürgi- Schmelz / Gabriel Gamez, Regula Dettling-Ott, Katharina Eggenberger, Astrid Epiney / Annekathrin Meier / Andrea Egbuna-Joss, Alice Göttler / Nina Grolimund, Dieter W. Grossen / Claire de Coulon, Tobias Jaag / Magda Zihlmann, Thomas Jaussi / Roland Schweighauser / Olivier Gehriger / Sibylle Blättler, Roland A. Müller, Hans Nater / Michael Tuchschmid, Wolfgang Portmann, Richard Senti, Andreas Kellerhals / Roger Zäch, Daniel Thürer / Carolin Hillemanns, Dirk Trüten / Florian Hanslik, Catrin Walser, Verna Weber, Rolf H. Weber, Rolf H. Weber / Max Friedli, Wolfgang Wohlers, 2007 – CHF 278.–

Der technische Fortschritt schafft neue Gelegenheiten für Kriminalität. Man denke nur an Hacking, Datenbeschädigung, Trojanische Pferde und andere Schadsoftware im Internet. Auch im Alltag werden immer häufiger technische Hilfsmittel zu kriminellen Zwecken eingesetzt wie beispielsweise Drohnen mit hochauflösenden Kameras, Miniwanzen und andere Sensoren zur Aufzeichnung von vertraulichen Bildern und Ton. Die Technik ist aber auch ein Hilfsmittel für die Kriminalprävention. Zu nennen sind etwa bauliche Massnahmen an Häusern, Videoaufzeichnungen in Trams, Bussen oder der Eisenbahn, automatische Suchläufe nach illegalen Inhalten im Internet, Aufklärungsdrohnen, elektronische Fussfesseln und Apps zur Registrierung von verdächtigem Verhalten. Sie alle können zur Verhinderung von Straftaten und zur Beweissicherung eingesetzt werden. Mit der zunehmenden Verfügbarkeit von Daten sind auch neue Auswertungsmethoden (machine learning, big data analysis) möglich, die zu individuellen oder räumlichen Prognosen eingesetzt werden. Das neue Zauberwort lautet: Computational Criminology. Diese Sammlung von Aufsätzen beschreibt die Vielfalt der Einsatzmöglichkeiten neuer Technologie im Dienste der Kriminalprävention. Anwendungsbeispiele erläutern den gegenwärtigen Stand der Umsetzung in der Praxis.

Zu den Autoren des Bandes gehören:

Dr. Ulf Blanke
Ladina Cavelti
Dr. Ulrich Schimpel
Dr. Jasmine Stössel
Thomas Wenk
Bettina Zahnd

buch & netz